



*See inside to learn how to obtain your CNSS
Certification and CPE credits.....*

NSA & CNSS Certified.....

...IT Security Training for NSTISSI No. 4013!

Web-Based IT Security Training Solution

Course Catalog

February 2003

Karta Technologies, Inc.

www.karta.com

Capital Area Office

1501 Lee Highway, Suite 200
Rosslyn, VA 22209

Sonny Kakar
(703) 469-2282
skakar@karta.com

Tracy Schoenleber
(703) 469-2080
(202) 215-0056
tschoenleber@karta.com

Corporate Headquarters

5555 Northwest Parkway
San Antonio, Texas 78249
1-800-725-2782

Aaron Bundschuh
(210) 582-3361
1-800-725-2782 ext 3361
abundschuh@karta.com

**Courses available for
CISSP/SSCP Continuing
Professional Education
Credits through (ISC)²**



© Copyright 2002
Karta Technologies, Inc.
ALL RIGHTS RESERVED.

Contents









Self-Paced e-Learning	iii
Catalog Description	iv
1.0 Introduction	1
1.1 Catalog Framework	2
1.2 National Security Agency (NSA)/Committee on National Security Systems (CNSS) Certification Procedures	3
1.3 Continuing Professional Education Credits for CISSPs and SSCPs	4
2.0 IT Security Tracks and Training Plans	5
2.1 Courses in the IT Security Library include:	5
2.2 Tracks and Training Plans	6
2.3 Information Security Tracks	7
Data Security (Technical)	7
Network Security (Technical)	7
Security Planning	8
Security Policy/Guidelines	8
2.4 Sample Training Plans	9
Information Security Officer (ISO)	10
IT Program Manager	11
Network/Systems Administrator	12
Database Administrator	13
Programmer/Systems Analyst	14
System Owner	15
System Designer/Developer	16
Technical Support Personnel	17
Data Center Manager	18
Systems Operations Personnel	19
Information Resources Manager	20
Information Resources Manager Officer	21
End User	21
Designated Approving Authority / Certification Reviewer	22
2.5 NIST Special Publication 800-16 Mapping	23
3.0 Course Descriptions	30
3.1 Advanced Local Network Security	31
3.2 Analyzing Network Security Plans	32
3.3 Authentication and Authorization in E-Commerce	32
3.4 Certification Authority	33
3.5 CGI and Encryption	33
3.6 Designing and Configuring Firewalls	34
3.7 Designing Local Network Security	34
3.8 Designing Remote Security Solutions	35
3.9 Designing WAN Security	35
3.10 Detecting Hackers	36
3.11 Distributed Security Planning	36
3.12 E-Commerce Payments Security	36
3.13 Encrypting File System (EFS)	37
3.14 Firewall Fundamentals	37
3.15 Fundamentals of Internet Security	38
3.16 Identifying Viruses	38

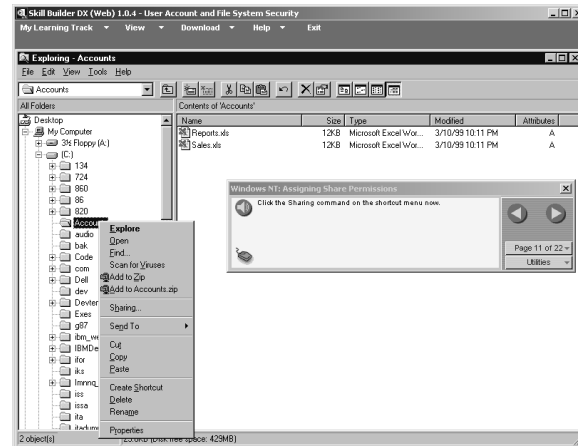
3.17	Implementing Network Security	39
3.18	Information Encryption with E-Commerce	39
3.19	IT Security Awareness (Beginning) *NEW COURSE*	40
3.20	IT Security Awareness (Intermediate)	40
3.21	Integrating Windows NT and NetWare	40
3.22	Introduction to Network Security Planning for Windows 2000	41
3.23	Intrusion Detection	41
3.24	Java Servlet Security	41
3.25	JavaBeans Security	42
3.26	Licensing and Security for Novell NetWare 5	43
3.27	Log Analysis	43
3.28	Managing Network Security	44
3.29	Managing Security for Microsoft Internet Explorer	44
3.30	Managing User Security for Windows NT	45
3.31	Microsoft Proxy Server Security Features	45
3.32	Network Security Policy	46
3.33	Network Vulnerabilities and Prevention	46
3.34	Overview of E-Commerce Security	46
3.35	Overview of Java Security	47
3.36	Overview of Network Security for Windows 2000	47
3.37	Pretty Good Privacy	47
3.38	Principles of Operating Systems Security	47
3.39	Recovering Data for Windows 2000	48
3.40	Remote Access Service for Window NT	48
3.41	Risk Management	49
3.42	Risks Assessment	49
3.43	Securing Access to Partners	49
3.44	Securing an Automated Information System	50
3.45	Securing Cisco Routers	50
3.46	Securing Communication Channels	51
3.47	Securing Internet Access with Firewalls	51
3.48	Securing Local Area Networks	52
3.49	Securing Network Access	52
3.50	Securing Network Resources	53
3.51	Securing Remote Connectivity	54
3.52	Security Auditing	54
3.53	Security Firewalls for E-Commerce	55
3.54	Security Over Internet Protocol (IPSec)	55
3.55	Security Strategies: External	56
3.56	Security Strategies: Internal	56
3.57	Session Beans: Development and Security	57
3.58	TCP/IP Security	57
3.59	Transaction Management	58
3.60	Troubleshooting Local Area Networks	59
3.61	Understanding Kerberos	59
3.62	User Account and File System Security	60
3.63	Virus Protection and Recovery	60
3.64	Windows 2000 Security Management	60
3.65	Windows NT Networking: Multiple Domains	61
4.0	Glossary	62








Self-Paced e-Learning

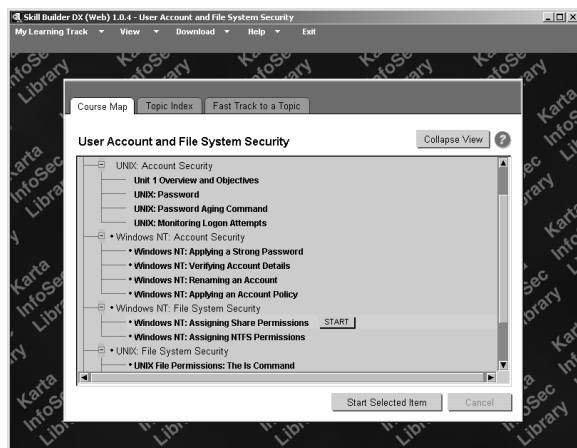
Bring IT Security Training to your desktop and organization...

Learn exactly what you need, when you need it!




-  Trains technical staff to respond to and prevent security threats
-  Meet requirements set forth by the Computer Security Act of 1987
-  Use the training plans to improve your security rating by including it as part of your FISMA response
-  Curriculum received NSA and CNSS Certification by meeting National Standards for NSTISSI No. 4013 through 2006!
-  Continuing Professional Education credits available for CISSP/SSCP through (ISC)²
-  Based on federal guidelines and mapped to NIST SP 800-16 in order to create 18 integrated training plans
-  Ensures consistent training across the organization, which focuses on IT Security job functions, roles and responsibilities
-  Comprehensive rollout/internal assistance to managers and training coordinators – an important key to success



-  Standard reports are available to show course completion, progress, and assessment scores
-  Web Site Hosting, Administration, Custom Web Site Branding, and Implementation Support
-  Browser Playable, with no plug-ins required (Microsoft Internet Explorer and Netscape Navigator, Version 4.0)
-  Help Desk Support 24/7
-  Audio with text
-  Pre and Post Assessments, exercises, simulations, and quizzes built into each course
-  Expert mentoring available 24/7 to answer your IT Security related questions



Karta's solution also includes the ability to:

-  Develop custom training courses
-  Provide ongoing marketing to increase usage and acceptance
-  Provide full e-Learning consulting services

Catalog Description

Section 1 provides an overview of Karta's IT Security Training Solution, its origin and intent. Information about receiving an NSA/CNSS Certification and Continuing Education Credits are also located in this section.

Section 2 relates specific courses to the training plans associated with various roles/users (ISO, Program Manager, Database Administrator, System Owner, Etc.) responsible for IT Security. It further organizes them by Core Competency (e.g., Firewall Fundamentals, Detecting Hackers, Security Auditing, etc.), Course Level (Beginning, Intermediate, and Advanced) and Functional Track (e.g., Data Security, Network Security, Security Planning, and Security Policy/ Guidelines).

The four "Learning Tracks" that have been defined in an effort to simplify Learning Plan management include:

- **Data Security:** The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.
- **Network Security:** Protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance that the network performs its critical functions correctly and there are no harmful side effects.
- **Security Guidelines and Policy:** Specifies the actions, prohibitions, and likely responses/judgments associated with network services, their intended usage and/or infractions thereof.
- **Security Planning:** Proactively identifies resources that need protection and individuals/groups they need protection from, assesses and addresses threats.

NIST Special Publication 800-16 Mapping Information:

The courses in the IT Security Library were designed to meet the requirements specified by the NIST Special Publication 800-16. The process used to map the courses to the requirements is also included in Section 2.

Section 3 of this document provides a detailed description for every course in the library, including prerequisites (when applicable).

Section 4 of this document includes a glossary of terms that are used throughout the document.

IT Security Training Solution

1.0 Introduction

Dramatic increases in computer interconnectivity, especially in use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. In addition to the benefits of improved collaboration; unlimited, shared access to information; and real-time business and financial transactions, etc., widespread interconnectivity poses significant risks to our computer systems and, more importantly, to the critical operations and infrastructures they support. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of confidential information.

Evaluations published by the GAO "Audits on Computer Security", since July 1999, continue to show that federal computer systems are riddled with weaknesses that place critical operations and assets at risk. To address the "high-risk areas that touch virtually every major aspect of government operations", GAO identified underlying factors, and NIST responded by publishing its Special Publication 800-16, which specifies the "Role-and Performance-based Model" for IT Security Training requirements. As a result, NIST's comprehensive approach to IT Security Training has been adopted by many government agencies.

To standardize the content and delivery of IT Security Training within government entities, various classroom and computer-based training programs were instituted and/or evaluated, with varying degrees of success. The most popular method of training, classroom-based, requires students to attend instructor-led courses and spend time away from the office. This often results in a conflict between work time and learning time, with learning usually losing out. In an on-demand, e-Learning environment, learning can be fully integrated with a wide range of job functions, including problem solving, Just-In-Time (JIT) computer application training, communications, and professional development.

"The brave new world of net delivered training is exciting and real. We strongly believe that it is not a replacement for classroom instruction but a critical extension of learning services. CEO's aren't viewing On-Line Learning as a way to improve training. They are focusing on a critical shift in how their organization will provide support for performance to their employees."

— Elliott Masie, President of the MASIE Center

By way of definition, e-Learning includes all internet-based training, either self-paced (asynchronous), or instructor-led (synchronous). e-Learning presents the opportunity to drastically improve the effectiveness and efficiency of training; fully integrates organizational training programs with tracking and career development planning; provides a relatively easy, cost-effective opportunity to measure return on investment; and links training investments to the impact on the strategic bottom line. In short, the efficiencies gained by e-Learning in time, tuition, and student effort are more than enough to justify a wide-scale deployment of an e-Learning program. And that's exactly what Karta has done!

To address the training requirements specified in federal guidance and standards documents as well as agency-specific requirements, Karta enlisted (and continues to work with) Information Security Officers from departments and agencies throughout the government to determine the range and depth of topics to be addressed. Moreover, to minimize costs and maximize value, Karta has teamed with several core Application Service Providers to provide a "1-stop shop" for quality IT Security Training, and offers it via an on-demand, e-Learning platform which is available 24 hours a day and fully integrated with a wide range of complementary IT Security related job functions.

Karta offers an extensive IT Security Training Library (e.g., more than 64 courses) that support training needs for a variety of roles, competency levels and disciplines. More courses will be added to the library over time, as others are modified and/or retired, in response to industry changes and customer requirements.

1.1 Catalog Framework

The courses detailed in this catalog are based on the NIST Special Publication 800-16, which provides a framework for determining the training needs of particular categories of employees and contractors involved with sensitive but unclassified computer systems. This framework includes the IT Security Training requirements appropriate for today's distributed computing environment and provides flexibility for extensions to accommodate future technologies and the related risk management decisions.

The learning approach presented in this catalog is designed to facilitate "results-based" learning.

- It focuses on job functions, roles and responsibilities specific to individuals, not job titles; and it recognizes that individuals have unique backgrounds, and therefore, different levels of understanding.
- It provides an integrated framework (planning tool) to identify training needs throughout the workforce, which can be used to ensure that everyone receives appropriate training.

This is accomplished by using standards-based course mappings, sample curriculums, and easy to use tables that ensure that the roles and performance-based training criteria are being met for every course and every student.





1.2 National Security Agency (NSA)/Committee on National Security Systems (CNSS) Certification Procedures

Karta's IT Security curriculum has been certified by the Committee on National Systems Security (CNSS) and the National Security Agency (NSA) for meeting national education and training requirements for NSTISSI No. 4013 (System Administration).

Karta participated in the Information Assurance Courseware Evaluation Process established by the CNSS and the NSA and met national education and training requirements in Information Assurance. The process systematically assesses the degree to which the various institution curriculums satisfy the NSTISSI standards. The certified institutions are now authorized to issue certificates to students completing the courses used in the program.

What is a CNSS/NSA Certification?

CNSS and NSA have developed a nationally recognized certification program based on NSTISSI standards. The process certifies institutions as meeting all of the elements of a specific standard with a designated set of courseware. Karta received notification from the National INFOSEC Education and Training Program (NIETP) that their IT Security Training Solution mapped 100% to the CNSS National Standards for NSTISSI No. 4013 through academic year 2006.

What are the steps to receive a CNSS/NSA Certification from Karta Technologies, Inc.?

1. Gain access to Karta's web based IT Security Library by contacting CNSScertification@karta.com.
2. Complete all 26 courses/50 hours of training needed for certification (certification course requirements can be found on the Karta website at www.karta.com).
3. Students must receive a 70% or higher on all of the Post Assessments located at the end of each course.
4. Submit the online application form to CNSScertification@karta.com when you have completed all 26 courses and received the passing score on all post assessments.
5. Karta will generate a report to confirm that the course requirements and assessment scores have been met.
6. Karta will issue a CNSS/NSA certificate with the CNSS seal to each individual for completing national level standards for NSTISSI No. 4013.
7. Start reaping the benefits of being a CNSS certified IT Security Professional!

1.3 Continuing Professional Education Credits for CISSPs and SSCPs

Karta Technologies, Inc. and (ISC)² have joined forces as Educational Partners. Individuals holding Certified Information Systems Security Professional (CISSP) or System Security Certified Practitioner (SSCP) can earn one Continuing Professional Education (CPE) credit for each hour of education accomplished in Karta's IT Security Library from (ISC)². Individuals can take any of the courses found in Karta's IT Security Library for credit. To learn more about and register for access to the IT Security Library, visit the Karta's Web site at www.karta.com or email cissp@karta.com.

What are the steps to receive CPE credits using Karta's Web Based IT Security Courses towards maintaining the CISSP and SSCP Certifications?

1. Gain access to Karta's online library by emailing Karta at cissp@karta.com.
2. Determine which courses you would like to take towards your CPE credits.
3. Remember you can earn one CPE credit for each hour of education accomplished.
4. When a course(s) is completed, fill out the registration form and email to cissp@karta.com. Karta will automatically send a report to (ISC)² to inform them of your completion (students do not need to report CPE credit completion directly to (ISC)²).

2.0 IT Security Tracks and Training Plans

2.1 Courses in the IT Security Library include:

- Advanced Local Network Security
- Analyzing Network Security Plans
- Authentication and Authorization in E-Commerce
- Certification Authority
- CGI and Encryption
- Designing and Configuring Firewalls
- Designing Local Network Security
- Designing Remote Security Solutions
- Designing WAN Security
- Detecting Hackers
- Distributed Security Planning
- E-Commerce Payments Security
- Encrypting File Systems (EFS)
- Firewall Fundamentals
- Fundamentals of Internet Security
- Identifying Viruses
- Implementing Network Security
- Information Encryption with E-Commerce
- IT Security Awareness – Beginning
- IT Security Awareness - Intermediate
- Integrating Windows NT and Novell NetWare
- Introduction to Network Security Planning for Windows 2000
- Intrusion Detection
- Java Servlet Security
- Java Beans Security
- License and Security for Novell NetWare 5
- Log Analysis
- Managing Network Security
- Managing Security for Microsoft Internet Explorer
- Managing User Security for Windows NT
- Microsoft Proxy Server Security Features
- Network Security Policy
- Network Vulnerabilities and Prevention
- Overview of E-Commerce Security
- Overview of Java Security
- Overview of Network Security for Windows 2000
- Pretty Good Privacy
- Principles of Operating Systems Security
- Recovering Data for Windows 2000
- Remote Access Service for Windows NT
- Risk Management
- Risks Assessment
- Securing Access to Partners
- Securing an Automated Information System
- Securing Cisco Routers
- Securing Communication Channels
- Securing Internet Access with Firewalls
- Securing Local Area Networks
- Securing Network Access
- Securing Network Resources
- Securing Remote Connectivity
- Security Auditing
- Security Firewalls for E-Commerce
- Security Over Internet Protocol (IPSec)
- Security Strategies: External
- Security Strategies: Internal
- Session Beans: Development and Security
- TCP/IP Security
- Transaction Management
- Trouble Shooting Local Area Networks
- Understanding Kerberos
- User Account and File System Security
- Virus Protection and Recovery
- Windows 2000 Security Management
- Windows NT Networking: Multiple Domain

2.2 Tracks and Training Plans

Over time, individuals acquire different roles relative to the use of IT within an organization, or as they make a career move to a different organization. Therefore, a roles- and performance-based approach to personal and career development is necessary, based on the individual's knowledge, experience, job requirements and interests.

Karta's IT Security Training Solution addresses this issue, and promotes an "individualized" approach to training. The curriculum and skills mapping matrix can be used to facilitate/augment the existing training plans, yielding a high value, streamlined learning experience customized for each student's particular learning needs. In fact, this program also doubles as an electronic performance support system, in that provides Just-In-Time access to the right information, at the right place and time.

To help IT Security Officers (and their constituents) create and manage a robust security training plan, Karta has provided training plans for 18 different roles, ranging from IT Security Officer (ISO) to basic End User. Turn to page 8 to view the sample training plans associated with each.

The courses have also been organized into four different tracks, each associated with various aspects of IT Security Training. They are as follows:

- **Data Security:** The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.
- **Network Security:** Protection of networks and their services from unauthorized modification, destruction, or disclosure. It provides assurance the network performs its critical functions correctly and there are no harmful side effects.
- **Security Guidelines and Policy:** Specify the actions, prohibitions and likely responses/judgments associated with network services, their intended usage and/or infractions thereof.
- **Security Planning:** Proactively identifies resources that need protection and individuals/groups they need protection from, assesses and addresses threats.

2.3 Information Security Tracks

Although the courses have been organized into four tracks—Data Security, Network Security, Security Planning, and Security Policy/Guidelines—they can be taken in any order, provided the necessary course prerequisites have been met. Refer to Part 3 for a detailed list and description of courses.

Data Security (Technical)

LEVEL	COURSE
Beginning	IT Security Awareness (Beginning)
	Overview of Java Security
Intermediate	CGI and Encryption
	Fundamentals of Internet Security
	Information Encryption with E-Commerce
	IT Security Awareness (Intermediate)
Advanced	Java Servlet Security
	JavaBeans Security
	Session Beans: Development and Security

Network Security (Technical)

LEVEL	COURSE
Beginning	Firewall Fundamentals
	IT Security Awareness (Beginning)
	Overview of Network Security for Windows 2000
	Security Firewalls for E-Commerce
Intermediate	Designing and Configuring Firewalls
	Designing WAN Security
	Fundamentals of Internet Security
	Implementing Network Security
	Integrating Windows NT and Novell NetWare
	IT Security Awareness (Intermediate)
	License and Security for Novell NetWare 5
	Managing Network Security
	Network Vulnerabilities and Prevention
	Recovering Data for Windows 2000
	Securing Local Area Networks
	Securing Network Access
	Securing Network Resources
	Securing Remote Connectivity
Advanced	Troubleshooting Local Area Networks
	Advanced Local Network Security
	Designing Local Network Security
	Intrusion Detection
	Log Analysis
	Remote Access Service for Windows NT
	Securing Access to Partners
	Securing Cisco Routers
	TCP/IP Security
	Windows NT Networking: Multiple Domains

Security Planning

LEVEL	COURSE
Beginning	IT Security Awareness (Beginning)
	Introduction to Network Security Planning for Windows 2000
Intermediate	Analyzing Network Security Plans
	Designing Remote Security Solutions
	Detecting Hackers
	Distributed Security Planning
	Fundamentals of Internet Security
	IT Security Awareness (Intermediate)
	Securing an Automated Information System

Security Policy/Guidelines

LEVEL	COURSE
Beginning	Identifying Viruses
	IT Security Awareness (Beginning)
	Managing Security for Microsoft Internet Explorer
	Overview of E-Commerce Security
	Securing Internet Access with Firewalls
	Security Firewalls for E-Commerce
	Virus Protection and Recovery
Intermediate	Authentication and Authorization in E-Commerce
	Certification Authority
	Designing Local Network Security
	E-Commerce Payments Security
	Encrypting File Systems (EFS)
	Fundamentals of Internet Security
	IT Security Awareness (Intermediate)
	Managing User Security for Windows NT
	Microsoft Proxy Server Security Features
	Network Security Policy
	Overview of Java Security
	Pretty Good Privacy
	Principles of Operating Systems Security
	Risk Management
	Risks Assessment
	Securing Communication Channels
	Security Over Internet Protocol (IPSec)
	Security Strategies: External
	Security Strategies: Internal
	Transaction Management
	Understanding Kerberos
	User Account and File System Security
	Windows 2000 Security Management
Advanced	Intrusion Detection
	Security Auditing

2.4 Sample Training Plans

This section of the course catalog outlines the different roles (or users) that are responsible for IT resources. Each role has been associated with the corresponding course recommendations (sample training plans), based on core competencies (Beginning, Intermediate, and Advanced) and tracks, such as Data Security, Network Security, Security Planning, and Security Policy/Guidelines.

Sample Training Plans and corresponding page numbers are as follows:

3.3.1	Information Security Officer	10
3.3.2	IT Program Manager.....	11
3.3.3	Network/Systems Administrator.....	12
3.3.4	Database Administrator (DBA)	13
3.3.5	Programmer/Systems Analyst	14
3.3.6	System Owner	15
3.3.7	Systems Designer/Developer	16
3.3.8	Technical Support Personnel.....	17
3.3.9	Data Center Manager	18
3.3.10	Systems Operations Personnel	19
3.3.11	Information Resources Manager	20
3.3.12	Information Resources Manager Official	21
3.3.13	End Users	21
3.3.14	Designated Approving Authority (DAA) / Certification Reviewer	22

Information Security Officer (ISO)

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99030	Identifying Viruses	B	Security Policy/Guidelines	2
99055	Overview of E-Commerce Security	B	Security Policy/Guidelines	1
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99056	Securing Internet Access with Firewalls	B	Security Policy/Guidelines	1
99027	Introduction to Network Security Planning for	B	Security Planning	2
99050	Firewall Fundamentals	B	Network Security	1
99007	Overview of Network Security for Windows	B	Network Security	1
99002	Security Firewalls for E-Commerce	B	Network Security	1
99067	IT Security Awareness (Beginning)	B	All	.5
99032	IT Security Awareness (Intermediate)	I	All	1
99004	Authentication and Authorization in E-	I	Security Policy/Guidelines	1
99019	Certification Authority	I	Security Policy/Guidelines	2
99005	E-Commerce Payments Security	I	Security Policy/Guidelines	1
99034	Managing User Security for Windows NT	I	Security Policy/Guidelines	2
99040	Microsoft Proxy Server Security Features	I	Security Policy/Guidelines	2
99009	Network Security Policy	I	Security Policy/Guidelines	1
99006	Overview of Java Security	I	Security Policy/Guidelines	1
99029	Pretty Good Privacy	I	Security Policy/Guidelines	2
99044	Principles of Operating Systems Security	I	Security Policy/Guidelines	1
99047	Risk Management	I	Security Policy/Guidelines	2
99046	Risks Assessment	I	Security Policy/Guidelines	1
99057	Securing Communication Channels	I	Security Policy/Guidelines	2
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99026	Security Strategies: External	I	Security Policy/Guidelines	2
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99062	Transaction Management	I	Security Policy/Guidelines	2
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99045	User Account and File System Security	I	Security Policy/Guidelines	2
99053	Windows 2000 Security Management	I	Security Policy/Guidelines	1
99017	Analyzing Network Security Plans	I	Security Planning	3
99058	Designing Remote Security Solutions	I	Security Planning	2
99052	Detecting Hackers	I	Security Planning	1
99025	Distributed Security Planning	I	Security Planning	2
99016	Securing and Automated Information System	I	Security Planning	2
99038	Fundamentals of Internet Security	I	All	3
99059	Designing WAN Security	I	Network Security	2
99031	Implementing Network Security	I	Network Security	2
99023	Managing Network Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99049	Securing Network Resources	I	Network Security	2
99010	Troubleshooting Local Area Networks	I	Network Security	2
99041	Intrusion Detection	A	Security Policy/Guidelines	3
99043	Security Auditing	A	Security Policy/Guidelines	1
99066	Java Servlet Security	A	Data Security	1
99063	JavaBeans Security	A	Data Security	3
99065	Session Beans: Development and Security	A	Data Security	2
99061	Advanced Local Network Security	A	Network Security	3
99060	Designing Local Network Security	A	Network Security	4
99042	Log Analysis	A	Network Security	1
99054	Securing Access to Partners	A	Network Security	2
99048	TCP/IP Security	A	Network Security	1
99033	Managing Security for Microsoft Internet	BO	Security Policy/Guidelines	2
99014	Encrypting File Systems (EFS)	IO	Security Policy/Guidelines	1
99013	CGI and Encryption	IO	Data Security	1
99003	Information Encryption with E-Commerce	IO	Data Security	2
99051	Designing and Configuring Firewalls	IO	Network Security	1
99036	Integrating Windows NT and Novell NetWare	IO	Network Security	1
99037	License and Security for Novell NetWare 5	IO	Network Security	2
99022	Recovering Data for Windows 2000	IO	Network Security	2
99018	Securing Local Area Networks	IO	Network Security	2
99020	Securing Network Access	IO	Network Security	2
99011	Securing Remote Connectivity	IO	Network Security	3
99039	Remote Access Service for Windows NT	AO	Network Security	2
99064	Securing Cisco Routers	AO	Network Security	3
99035	Windows NT Networking (Multiple Domains)	AO	Network Security	2

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional,
AO=Advanced Optional

IT Program Manager

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99033	Managing Security for Microsoft Internet Explorer	B	Security Policy/Guidelines	2
99055	Overview of E-Commerce Security	B	Security Policy/Guidelines	1
99056	Securing Internet Access with Firewalls	B	Security Policy/Guidelines	1
99050	Firewall Fundamentals	B	Network Security	1
99067	IT Security Awareness (Beginning)	B	All	.5
99032	IT Security Awareness (Intermediate)	I	All	1
99014	Encrypting File Systems (EFS)	I	Security Policy/Guidelines	1
99009	Network Security Policy	I	Security Policy/Guidelines	1
99044	Principles of Operating Systems Security	I	Security Policy/Guidelines	1
99047	Risk Management	I	Security Policy/Guidelines	2
99046	Risks Assessment	I	Security Policy/Guidelines	1
99057	Securing Communication Channels	I	Security Policy/Guidelines	2
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99026	Security Strategies: External	I	Security Policy/Guidelines	2
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99062	Transaction Management	I	Security Policy/Guidelines	2
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99053	Windows 2000 Security Management	I	Security Policy/Guidelines	1
99017	Analyzing Network Security Plans	I	Security Planning	3
99058	Designing Remote Security Solutions	I	Security Planning	2
99052	Detecting Hackers	I	Security Planning	1
99025	Distributed Security Planning	I	Security Planning	2
99059	Designing WAN Security	I	Network Security	2
99031	Implementing Network Security	I	Network Security	2
99023	Managing Network Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99018	Securing Local Area Networks	I	Network Security	2
99049	Securing Network Resources	I	Network Security	2
99011	Securing Remote Connectivity	I	Network Security	3
99038	Fundamentals of Internet Security	I	All	3
99061	Advanced Local Network Security	A	Network Security	3
99060	Designing Local Network Security	A	Network Security	4
99041	Intrusion Detection	A	Network Security	3
99054	Securing Access to Partners	A	Network Security	2
99035	Windows NT Networking: Multiple Domains	A	Network Security	2
99063	JavaBeans Security	A	Data Security	3
99065	Session Beans: Development and Security	A	Data Security	2
99051	Designing and Configuring Firewalls	IO	Network Security	1
99036	Integrating Windows NT & Novell NetWare 5	IO	Network Security	1
99037	License and Security for Novell NetWare 5	IO	Network Security	2
99022	Recovering Data for Windows 2000	IO	Network Security	2
99010	Troubleshooting Local Area Networks	IO	Network Security	2
99042	Log Analysis	AO	Network Security	1
99064	Securing Cisco Routers	AO	Network Security	3
99039	Remote Access Service for Windows NT	AO	Network Security	2

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional, AO=Advanced Optional

Network/Systems Administrator

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99030	Identifying Viruses	B	Security Policy/Guidelines	2
99033	Managing Security for Microsoft Internet Explorer	B	Security Policy/Guidelines	2
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99007	Overview of Network Security for Windows 2000	B	Network Security	1
99067	IT Security Awareness (Beginning)	B	All	.5
99032	IT Security Awareness (Intermediate)	I	All	1
99019	Certification Authority	I	Security Policy/Guidelines	2
99014	Encrypting File Systems (EFS)	I	Security Policy/Guidelines	1
99034	Managing User Security for Windows NT	I	Security Policy/Guidelines	2
99040	Microsoft Proxy Server Security Features	I	Security Policy/Guidelines	2
99009	Network Security Policy	I	Security Policy/Guidelines	1
99029	Pretty Good Privacy	I	Security Policy/Guidelines	2
99047	Risk Management	I	Security Policy/Guidelines	2
99057	Securing Communication Channels	I	Security Policy/Guidelines	2
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99053	Windows 2000 Security Management	I	Security Policy/Guidelines	1
99058	Designing Remote Security Solutions	I	Security Planning	2
99052	Detecting Hackers	I	Security Planning	1
99013	CGI and Encryption	I	Data Security	1
99038	Fundamentals of Internet Security	I	All	3
99031	Implementing Network Security	I	Network Security	2
99023	Managing Network Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99022	Recovering Data for Windows 2000	I	Network Security	2
99018	Securing Local Area Networks	I	Network Security	2
99020	Securing Network Access	I	Network Security	2
99011	Securing Remote Connectivity	I	Network Security	3
99010	Troubleshooting Local Area Networks	I	Network Security	2
99041	Intrusion Detection	A	Security Policy/Guidelines	3
99043	Security Auditing	A	Security Policy/Guidelines	1
99061	Advanced Local Network Security	A	Network Security	3
99060	Designing Local Network Security	A	Network Security	4
99042	Log Analysis	A	Network Security	1
99039	Remote Access Service for Windows NT	A	Network Security	2
99048	TCP/IP Security	A	Network Security	1
99055	Overview of E-Commerce Security	BO	Security Policy/Guidelines	1
99027	Introduction to Network Security Planning for Windows 2000	BO	Security Planning	2
99050	Firewall Fundamentals	BO	Network Security	1
99004	Authentication and Authorization in E-Commerce	IO	Security Policy/Guidelines	1
99005	E-Commerce Payments Security	IO	Security Policy/Guidelines	1
99006	Overview of Java Security	IO	Security Policy/Guidelines	1
99046	Risks Assessment	IO	Security Policy/Guidelines	1
99026	Security Strategies: External	IO	Security Policy/Guidelines	2
99017	Analyzing Network Security Plans	IO	Security Planning	3
99016	Securing and Automated Information System	IO	Security Planning	2
99003	Information Encryption with E-Commerce	IO	Data Security	1
99051	Designing and Configuring Firewalls	IO	Network Security	1
99059	Designing WAN Security	IO	Network Security	2
99036	Integrating Windows NT and Novell NetWare	IO	Network Security	1
99037	License and Security for Novell NetWare 5	IO	Network Security	2
99066	Java Servlet Security	AO	Data Security	1
99063	JavaBeans Security	AO	Data Security	3
99065	Session Beans: Development and Security	AO	Data Security	2
99054	Securing Access to Partners	AO	Network Security	2
99064	Securing Cisco Routers	AO	Network Security	3

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional, AO=Advanced Optional

Database Administrator

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99030	Identifying Viruses	B	Security Policy/Guidelines	2
99067	IT Security Awareness (Beginning)	B	All	.5
99033	Managing Security for Microsoft Internet Explorer	B	Security Policy/Guidelines	2
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99027	Introduction to Network Security Planning for Windows 2000	B	Security Planning	2
99007	Overview of Network Security for Windows 2000	B	Network Security	1
99006	Overview of Java Security	B	Data Security	1
99038	Fundamentals of Internet Security	I	All	3
99032	IT Security Awareness (Intermediate)	I	All	1
99004	Authentication and Authorization in E-Commerce	I	Security Policy/Guidelines	1
99019	Certification Authority	I	Security Policy/Guidelines	2
99005	E-Commerce Payments Security	I	Security Policy/Guidelines	1
99040	Microsoft Proxy Server Security Features	I	Security Policy/Guidelines	2
99009	Network Security Policy	I	Security Policy/Guidelines	1
99029	Pretty Good Privacy	I	Security Policy/Guidelines	2
99047	Risk Management	I	Security Policy/Guidelines	2
99046	Risks Assessment	I	Security Policy/Guidelines	1
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99026	Security Strategies: External	I	Security Policy/Guidelines	2
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99016	Securing and Automated Information System	I	Security Planning	2
99013	CGI and Encryption	I	Data Security	1
99003	Information Encryption with E-Commerce	I	Data Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99022	Recovering Data for Windows 2000	I	Network Security	2
99020	Securing Network Access	I	Network Security	2
99043	Security Auditing	A	Security Policy/Guidelines	1
99066	Java Servlet Security	A	Data Security	1
99063	JavaBeans Security	A	Data Security	3
99065	Session Beans: Development and Security	A	Data Security	2
99031	Implementing Network Security	IO	Network Security	2
99036	Integrating Windows NT and Novell NetWare	IO	Network Security	1
99023	Managing Network Security	IO	Network Security	2
99018	Securing Local Area Networks	IO	Network Security	2
99011	Security Remote Connectivity	IO	Network Security	3
99061	Advanced Local Network Security	AO	Network Security	3
99039	Remote Access Service for Windows NT	AO	Network Security	2
99064	Securing Cisco Routers	AO	Network Security	3
99048	TCP/IP Security	AO	Network Security	1

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional, AO=Advanced Optional

Programmer/Systems Analyst

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99033	Managing Security for Microsoft Internet Explorer	B	Security Policy/Guidelines	2
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99050	Firewall Fundamentals	B	Network Security	1
99067	IT Security Awareness (Beginning)	B	All	.5
99038	Fundamentals of Internet Security	I	All	3
99032	IT Security Awareness (Intermediate)	I	All	1
99029	Pretty Good Privacy	I	Security Policy/Guidelines	2
99044	Principles of Operating Systems Security	I	Security Policy/Guidelines	1
99047	Risk Management	I	Security Policy/Guidelines	2
99046	Risks Assessment	I	Security Policy/Guidelines	1
99026	Security Strategies: External	I	Security Policy/Guidelines	2
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99052	Detecting Hackers	I	Security Planning	1
99025	Distributed Security Planning	I	Security Planning	2
99016	Securing an Automated Information System	I	Security Planning	2
99022	Recovering Data for Windows2000	I	Network Security	2
99020	Securing Network Access	I	Network Security	2
99063	JavaBeans Security	A	Data Security	3
99042	Log Analysis	A	Network Security	1
99039	Remote Access Service for Windows NT	A	Network Security	2
99065	Session Beans: Development and Security	A	Data Security	2
99048	TCP/IP Security	A	Network Security	1
99035	Windows NT Networking: Multiple Domains	A	Network Security	2
99034	Managing User Security for Windows NT	IO	Security Policy/Guidelines	2
99040	Microsoft Proxy Server Security Features	IO	Security Policy/Guidelines	2
99045	User Account and File System Security	IO	Security Policy/Guidelines	2
99017	Analyzing Network Security Plans	IO	Security Planning	3
99058	Designing Remote Security Solutions	IO	Security Planning	2
99051	Designing and Configuring Firewalls	IO	Network Security	1
99037	License and Security for Novell NetWare 5	IO	Network Security	2
99023	Managing Network Security	IO	Network Security	2
99011	Securing Remote Connectivity	IO	Network Security	3
99010	Troubleshooting Local Area Networks	IO	Network Security	2
99061	Advanced Local Network Security	AO	Network Security	3
99060	Designing Local Network Security	AO	Network Security	4
99041	Intrusion Detection	AO	Network Security	3
99064	Securing Cisco Routers	AO	Network Security	3

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional,
AO=Advanced Optional

System Owner

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99067	IT Security Awareness (Beginning)	B	All	.5
99050	Firewall Fundamentals	B	Network Security	1
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99033	Managing Security for Microsoft Internet Explorer	B	Security Policy/Guidelines	2
99038	Fundamentals of Internet Security	I	All	3
99032	IT Security Awareness (Intermediate)	I	All	1
99051	Designing and Configuring Firewalls	I	Network Security	1
99031	Implementing Network Security	I	Network Security	2
99036	Integrating Windows NT and Novell NetWare	I	Network Security	1
99023	Managing Network Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99049	Securing Network Resources	I	Network Security	2
99017	Analyzing Network Security Plans	I	Security Planning	3
99058	Designing Remote Security Solutions	I	Security Planning	2
99052	Detecting Hackers	I	Security Planning	1
99016	Securing an Automated Information System	I	Security Planning	2
99060	Designing Local Network Security	I	Security Policy/Guidelines	4
99009	Network Security Policy	I	Security Policy/Guidelines	1
99044	Principles of Operating Systems Security	I	Security Policy/Guidelines	1
99047	Risk Management	I	Security Policy/Guidelines	3
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99045	User Account and File System Security	I	Security Policy/Guidelines	2
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99053	Windows 2000 Security Management	I	Security Policy/Guidelines	1
99041	Intrusion Detection	A	Network Security	3
99042	Log Analysis	A	Network Security	1
99054	Securing Access to Partners	A	Network Security	2
99048	TCP/IP Security	A	Network Security	1
99043	Security Auditing	A	Security Policy/Guidelines	1
99002	Security Firewalls for E-Commerce	BO	Network Security	2
99056	Securing Internet Access with Firewalls	BO	Security Policy/Guidelines	1
99055	Overview of E-Commerce Security	BO	Security Policy/Guidelines	1
99059	Designing WAN Security	IO	Network Security	2
99018	Securing Local Area Networks	IO	Network Security	2
99011	Securing Remote Connectivity	IO	Network Security	3
99025	Distributed Security Planning	IO	Security Planning	2
99019	Certification Authority	IO	Security Policy/Guidelines	2
99026	Security Strategies: External	IO	Security Policy/Guidelines	2
99057	Securing Communication Channels	IO	Security Policy/Guidelines	2
99062	Transaction Management	IO	Security Policy/Guidelines	2
99060	Designing Local Network Security	AO	Security Policy/Guidelines	4
99063	JavaBeans Security	AO	Data Security	3
99039	Remote Access Service for Windows NT	AO	Network Security	2
99064	Securing Cisco Routers	AO	Network Security	3
99065	Session Beans: Development and Security	AO	Data Security	2
99035	Windows NT Networking (Multiple Domains)	AO	Network Security	2

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional,
AO=Advanced Optional

System Designer/Developer

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99067	IT Security Awareness (Beginning)	B	All	.5
99050	Firewall Fundamentals	B	Network Security	1
99007	Overview of Network Security for Windows 2000	B	Network Security	1
99030	Identifying Viruses	B	Security Policy/Guidelines	2
99033	Managing Security for Microsoft Internet Explorer	B	Security Policy/Guidelines	2
99055	Overview of E-Commerce Security	B	Security Policy/Guidelines	1
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99038	Fundamentals of Internet Security	I	All	3
99032	IT Security Awareness (Intermediate)	I	All	1
99013	CGI and Encryption	I	Data Security	1
99031	Implementing Network Security	I	Network Security	2
99023	Managing Network Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99018	Securing Local Area Networks	I	Network Security	2
99049	Securing Network Resources	I	Network Security	2
99011	Securing Remote Connectivity	I	Network Security	3
99010	Troubleshooting Local Area Networks	I	Network Security	2
99017	Analyzing Network Security Plans	I	Security Planning	3
99052	Detecting Hackers	I	Security Planning	1
99025	Distributed Security Planning	I	Security Planning	2
99004	Authentication and Authorization in E-Commerce	I	Security Policy/Guidelines	1
99019	Certification Authority	I	Security Policy/Guidelines	2
99014	Encrypting File Systems (EFS)	I	Security Policy/Guidelines	1
99034	Managing User Security for Windows NT	I	Security Policy/Guidelines	2
99040	Microsoft Proxy Server Security Features	I	Security Policy/Guidelines	2
99009	Network Security Policy	I	Security Policy/Guidelines	1
99006	Overview of Java Security	I	Security Policy/Guidelines	1
99029	Pretty Good Privacy	I	Security Policy/Guidelines	2
99044	Principles of Operating Systems Security	I	Security Policy/Guidelines	1
99046	Risks Assessment	I	Security Policy/Guidelines	1
99047	Risk Management	I	Security Policy/Guidelines	2
99057	Securing Communication Channels	I	Security Policy/Guidelines	2
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99062	Transaction Management	I	Security Policy/Guidelines	2
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99045	User Account and File System Security	I	Security Policy/Guidelines	2
99053	Windows 2000 Security Management	I	Security Policy/Guidelines	1
99063	JavaBeans Security	A	Data Security	3
99066	Java Servlet Security	A	Data Security	1
99065	Session Beans: Development and Security	A	Data Security	2
99061	Advanced Local Network Security	A	Network Security	3
99054	Securing Access to Partners	A	Network Security	2
99048	TCP/IP Security	A	Network Security	1
99035	Windows NT Networking (Multiple Domains)	A	Network Security	2
99043	Security Auditing	A	Security Policy/Guidelines	1
99041	Intrusion Detection	A	Security Policy/Guidelines	3
99002	Security Firewalls for E-Commerce	BO	Network Security	2
99056	Securing Internet Access with Firewalls	BO	Security Policy/Guidelines	1
99003	Information Encryption with E-Commerce	IO	Data Security	2
99051	Designing and Configuring Firewalls	IO	Network Security	1
99059	Designing WAN Security	IO	Network Security	2
99036	Integrating Windows NT and Novell NetWare	IO	Network Security	1
99037	License and Security for Novell NetWare 5	IO	Network Security	2
99022	Recovering Data for Windows 2000	IO	Network Security	2
99020	Securing Network Access	IO	Network Security	2
99058	Designing Remote Security Solutions	IO	Security Planning	2
99016	Securing an Automated Information System	IO	Security Planning	2
99005	E-Commerce Payments Security	IO	Security Policy/Guidelines	1
99026	Security Strategies: External	IO	Security Policy/Guidelines	2
99060	Designing Local Network Security	AO	Network Security	4
99042	Log Analysis	AO	Network Security	1
99039	Remote Access Service for Windows NT	AO	Network Security	2
99064	Securing Cisco Routers	AO	Network Security	3

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional, AO=Advanced Optional

Technical Support Personnel

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99067	IT Security Awareness (Beginning)	B	All	.5
99007	Overview of Network Security for Windows 2000	B	Network Security	1
99027	Introduction to Network Security Planning for Windows 2000	B	Security Planning	2
99030	Identifying Viruses	B	Security Policy/Guidelines	2
99055	Overview of E-Commerce Security	B	Security Policy/Guidelines	1
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99032	IT Security Awareness (Intermediate)	I	All	1
99036	Integrating Windows NT and Novell NetWare	I	Network Security	1
99023	Managing Network Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99022	Recovering Data for Windows 2000	I	Network Security	2
99049	Securing Network Resources	I	Network Security	2
99011	Securing Remote Connectivity	I	Network Security	3
99052	Detecting Hackers	I	Security Planning	1
99016	Securing an Automated Information System	I	Security Planning	2
99019	Certification Authority	I	Security Policy/Guidelines	2
99005	E-Commerce Payments Security	I	Security Policy/Guidelines	1
99014	Encrypting File Systems (EFS)	I	Security Policy/Guidelines	1
99034	Managing User Security for Windows NT	I	Security Policy/Guidelines	2
99040	Microsoft Proxy Server Security Features	I	Security Policy/Guidelines	2
99009	Network Security Policy	I	Security Policy/Guidelines	1
99006	Overview of Java Security	I	Security Policy/Guidelines	1
99029	Pretty Good Privacy	I	Security Policy/Guidelines	2
99047	Risk Management	I	Security Policy/Guidelines	2
99057	Securing Communication Channels	I	Security Policy/Guidelines	2
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99026	Security Strategies: External	I	Security Policy/Guidelines	2
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99066	Java Servlet Security	A	Data Security	1
99063	JavaBeans Security	A	Data Security	3
99061	Advanced Local Network Security	A	Network Security	3
99042	Log Analysis	A	Network Security	1
99064	Securing Cisco Routers	A	Network Security	3
99048	TCP/IP Security	A	Network Security	1
99041	Intrusion Detection	A	Security Policy/Guidelines	3
99043	Security Auditing	A	Security Policy/Guidelines	2
99033	Managing Security for Microsoft Internet Explorer	BO	Security Policy/Guidelines	2
99013	CGI and Encryption	IO	Data Security	1
99003	Information Encryption with E-Commerce	IO	Data Security	2
99051	Designing and Configuring Firewalls	IO	Network Security	1
99037	License and Security for Novell NetWare 5	IO	Network Security	2
99018	Securing Local Area Networks	IO	Network Security	2
99020	Securing Network Access	IO	Network Security	2
99046	Risks Assessment	IO	Security Policy/Guidelines	1
99039	Remote Access Service for Windows NT	AO	Network Security	2
99065	Session Beans: Development and Security	AO	Data Security	2

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional,
AO=Advanced Optional

Data Center Manager

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99067	IT Security Awareness (Beginning)	B	All	.5
99050	Firewall Fundamentals	B	Network Security	1
99027	Introduction to Network Security Planning for Windows 2000	B	Security Planning	2
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99055	Overview of E-Commerce Security	B	Security Policy/Guidelines	1
99032	IT Security Awareness (Intermediate)	I	All	1
99003	Information Encryption with E-Commerce	I	Data Security	2
99031	Implementing Network Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99018	Securing Local Area Networks	I	Network Security	2
99020	Securing Network Access	I	Network Security	2
99052	Detecting Hackers	I	Security Planning	1
99019	Certification Authority	I	Security Policy/Guidelines	2
99034	Managing User Security for Windows NT	I	Security Policy/Guidelines	2
99040	Microsoft Proxy Server Security Features	I	Security Policy/Guidelines	2
99009	Network Security Policy	I	Security Policy/Guidelines	1
99006	Overview of Java Security	I	Security Policy/Guidelines	1
99029	Pretty Good Privacy	I	Security Policy/Guidelines	2
99044	Principles of Operating Systems Security	I	Security Policy/Guidelines	1
99047	Risk Management	I	Security Policy/Guidelines	2
99046	Risks Assessment	I	Security Policy/Guidelines	1
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99026	Security Strategies: External	I	Security Policy/Guidelines	2
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99061	Advanced Local Network Security	A	Network Security	3
99042	Log Analysis	A	Network Security	1
99048	TCP/IP Security	A	Network Security	1
99041	Intrusion Detection	A	Security Policy/Guidelines	3
99043	Security Auditing	A	Security Policy/Guidelines	1
99007	Overview of Network Security for Windows 2000	BO	Network Security	1
99033	Managing Security for Microsoft Internet Explorer	BO	Security Policy/Guidelines	2
99051	Designing and Configuring Firewalls	IO	Network Security	1
99036	Integrating Windows NT and Novell NetWare	IO	Network Security	1
99037	License and Security for Novell NetWare 5	IO	Network Security	2
99049	Securing Network Resources	IO	Network Security	2
99011	Securing Remote Connectivity	IO	Network Security	3
99016	Securing an Automated Information System	IO	Security Planning	2
99045	User Account and File System Security	IO	Security Policy/Guidelines	2
99066	Java Servlet Security	AO	Data Security	1
99063	JavaBeans Security	AO	Data Security	3
99065	Session Beans: Development and Security	AO	Data Security	2
99039	Remote Access Service for Windows NT	AO	Network Security	2
99064	Securing Cisco Routers	AO	Network Security	3
99035	Windows NT Networking (Multiple Domains)	AO	Network Security	2

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional, AO=Advanced Optional

Systems Operations Personnel

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99067	IT Security Awareness (Beginning)	B	All	.5
99050	Firewall Fundamentals	B	Network Security	1
99027	Introduction to Network Security Planning for Windows 2000	B	Security Planning	2
99033	Managing Security for Microsoft Internet Explorer	B	Security Policy/Guidelines	2
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99032	IT Security Awareness (Intermediate)	I	All	1
99051	Designing and Configuring Firewalls	I	Network Security	1
99031	Implementing Network Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99018	Securing Local Area Networks	I	Network Security	2
99020	Securing Network Access	I	Network Security	2
99049	Securing Network Resources	I	Network Security	2
99052	Detecting Hackers	I	Security Planning	1
99019	Certification Authority	I	Security Policy/Guidelines	2
99034	Managing User Security for Windows NT	I	Security Policy/Guidelines	2
99040	Microsoft Proxy Server Security Features	I	Security Policy/Guidelines	2
99009	Network Security Policy	I	Security Policy/Guidelines	1
99029	Pretty Good Privacy	I	Security Policy/Guidelines	2
99044	Principles of Operating Systems Security	I	Security Policy/Guidelines	1
99047	Risk Management	I	Security Policy/Guidelines	2
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99045	User Account and File System Security	I	Security Policy/Guidelines	2
99061	Advanced Local Network Security	A	Network Security	3
99042	Log Analysis	A	Network Security	1
99048	TCP/IP Security	A	Network Security	1
99041	Intrusion Detection	A	Security Policy/Guidelines	3
99043	Security Auditing	A	Security Policy/Guidelines	1
99007	Overview of Network Security for Windows 2000	BO	Network Security	1
99055	Overview of E-Commerce Security	BO	Security Policy/Guidelines	1
99003	Information Encryption with E-Commerce	IO	Data Security	2
99036	Integrating Windows NT and Novell NetWare	IO	Network Security	1
99037	License and Security for Novell NetWare 5	IO	Network Security	2
99011	Securing Remote Connectivity	IO	Network Security	3
99010	Troubleshooting Local Area Networks	IO	Network Security	2
99016	Securing an Automated Information System	IO	Security Planning	2
99006	Overview of Java Security	IO	Security Policy/Guidelines	1
99046	Risks Assessment	IO	Security Policy/Guidelines	1
99026	Security Strategies: External	IO	Security Policy/Guidelines	2
99066	Java Servlet Security	AO	Data Security	1
99063	JavaBeans Security	AO	Data Security	3
99065	Session Beans: Development and Security	AO	Data Security	2
99039	Remote Access Service for Windows NT	AO	Network Security	2
99064	Securing Cisco Routers	AO	Network Security	3

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional, AO=Advanced Optional

Information Resources Manager

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99067	IT Security Awareness (Beginning)	B	All	.5
99050	Firewall Fundamentals	B	Network Security	1
99056	Securing Internet Access with Firewalls	B	Security Policy/Guidelines	1
99024	Virus Protection and Recovery	B	Security Policy/Guidelines	1
99038	Fundamentals of Internet Security	I	All	3
99032	IT Security Awareness (Intermediate)	I	All	1
99059	Designing WAN Security	I	Network Security	2
99031	Implementing Network Security	I	Network Security	2
99018	Securing Local Area Networks	I	Network Security	2
99049	Securing Network Resources	I	Network Security	2
99010	Troubleshooting Local Area Networks	I	Network Security	2
99017	Analyzing Network Security Plans	I	Security Planning	3
99058	Designing Remote Security Solutions	I	Security Planning	2
99052	Detecting Hackers	I	Security Planning	1
99025	Distributed Security Planning	I	Security Planning	2
99016	Securing an Automated Information System	I	Security Planning	2
99060	Designing Local Network Security	I	Security Policy/Guidelines	4
99034	Managing User Security for Windows NT	I	Security Policy/Guidelines	2
99009	Network Security Policy	I	Security Policy/Guidelines	1
99044	Principles of Operating Systems Security	I	Security Policy/Guidelines	1
99047	Risk Management	I	Security Policy/Guidelines	2
99046	Risks Assessment	I	Security Policy/Guidelines	1
99057	Securing Communication Channels	I	Security Policy/Guidelines	2
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99045	User Account and File System Security	I	Security Policy/Guidelines	2
99053	Windows 2000 Security Management	I	Security Policy/Guidelines	1
99008	Understanding Kerberos	I	Security Policy/Guidelines	2
99061	Advanced Local Network Security	A	Network Security	3
99042	Log Analysis	A	Network Security	1
99041	Intrusion Detection	A	Security Policy/Guidelines	3
99043	Security Auditing	A	Security Policy/Guidelines	1
99002	Security Firewalls for E-Commerce	BO	Network Security	2
99055	Overview of E-Commerce Security	BO	Security Policy/Guidelines	1
99051	Designing and Configuring Firewalls	IO	Network Security	1
99036	Integrating Windows NT and Novell NetWare	IO	Network Security	1
99037	License and Security for Novell NetWare 5	IO	Network Security	2
99011	Securing Remote Connectivity	IO	Network Security	3
99004	Authentication and Authorization in E-Commerce	IO	Security Policy/Guidelines	1
99026	Security Strategies: External	IO	Security Policy/Guidelines	2
99062	Transaction Management	IO	Security Policy/Guidelines	2
99063	JavaBeans Security	AO	Data Security	3
99064	Securing Cisco Routers	AO	Network Security	3
99054	Securing Access to Partners	AO	Network Security	3
99035	Windows NT Networking (Multiple Domains)	AO	Network Security	2

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional, AO=Advanced Optional

Information Resources Manager Officer

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99067	IT Security Awareness (Beginning)	B	All	.5
99050	Firewall Fundamentals	B	Network Security	1
99032	IT Security Awareness (Intermediate)	I	All	1
99059	Designing WAN Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99017	Analyzing Network Security Plans	I	Security Planning	3
99058	Designing Remote Security Solutions	I	Security Planning	2
99052	Detecting Hackers	I	Security Planning	1
99060	Designing Local Network Security	I	Security Policy/Guidelines	4
99009	Network Security Policy	I	Security Policy/Guidelines	1
99044	Principles of Operating Systems Security	I	Security Policy/Guidelines	1
99047	Risk Management	I	Security Policy/Guidelines	2
99015	Security Over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99026	Security Strategies: External	I	Security Policy/Guidelines	2
99028	Security Strategies: Internal	I	Security Policy/Guidelines	1
99061	Advanced Local Network Security	A	Network Security	3
99054	Securing Access to Partners	A	Network Security	2
99041	Intrusion Detection	A	Security Policy/Guidelines	3
99043	Security Auditing	A	Security Policy/Guidelines	1
99055	Overview of E-Commerce Security	BO	Security Policy/Guidelines	1
99056	Securing Internet Access with Firewalls	BO	Security Policy/Guidelines	1
99051	Designing and Configuring Firewalls	IO	Network Security	1
99011	Securing Remote Connectivity	IO	Network Security	3
99010	Troubleshooting Local Area Networks	IO	Network Security	2
99053	Windows 2000 Security Management	IO	Security Policy/Guidelines	1
99042	Log Analysis	AO	Network Security	1
99064	Securing Cisco Routers	AO	Network Security	3
99063	JavaBeans Security	AO	Data Security	3

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced)

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional,
AO=Advanced Optional

End User

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99067	IT Security Awareness	B	All	.5
99032	IT Security Awareness	I	All	1

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional,
AO=Advanced Optional

Designated Approving Authority / Certification Reviewer

COURSE NUMBER	COURSE	LEVEL	TRACK	DURATION (HRS)
99007	Overview of Network Security for Windows 2000	B	Network Security	1
99027	Introduction to Network Security Planning for Windows 2000	B	Security Planning	2
99067	IT Security Awareness (Beginning)	B	All	.5
99032	IT Security Awareness (Intermediate)	I	All	1
99013	CGI and Encryption	I	Data Security	1
99003	Information Encryption with E-Commerce	I	Data Security	2
99031	Implementing Network Security	I	Network Security	2
99036	Integrating Windows NT and Novell NetWare	I	Network Security	1
99023	Managing Network Security	I	Network Security	2
99021	Network Vulnerabilities and Prevention	I	Network Security	2
99022	Recovering Data for Windows 2000	I	Network Security	2
99018	Securing Local Area Networks	I	Network Security	2
99020	Securing Network Access	I	Network Security	2
99011	Securing Remote Connectivity	I	Network Security	3
99017	Analyzing Network Security Plans	I	Security Planning	3
99016	Securing an Automated Information System	I	Security Planning	2
99019	Certification Authority	I	Security Policy/Guidelines	2
99040	Microsoft Proxy Server Security Features	I	Security Policy/Guidelines	2
99006	Overview of Java Security	I	Security Policy/Guidelines	1
99029	Pretty Good Privacy	I	Security Policy/Guidelines	2
99047	Risk Management	I	Security Policy/Guidelines	2
99046	Risks Assessment	I	Security Policy/Guidelines	1
99015	Security over Internet Protocol (IPSec)	I	Security Policy/Guidelines	2
99026	Security Strategies: External	I	Security Policy/Guidelines	2
99053	Windows 2000 Security Management	I	Security Policy/Guidelines	1
99005	E-Commerce Payments Security	I	Security Policy/Guidelines	1
99004	Authentication and Authorization in E-Commerce	I	Security Policy/Guidelines	1
99063	JavaBeans Security	A	Data Security	3
99066	Java Servlet Security	A	Data Security	1
99065	Session Beans: Development and Security	A	Data Security	2
99061	Advanced Local Network Security	A	Network Security	3
99041	Intrusion Detection	A	Network Security	3
99042	Log Analysis	A	Network Security	1
99039	Remote Access Service for Windows NT	A	Network Security	2
99054	Securing Access to Partners	A	Network Security	2
99064	Securing Cisco Routers	A	Network Security	3
99048	TCP/IP Security	A	Network Security	1
99043	Security Auditing	A	Security Policy/Guidelines	1

*Note: The shaded areas of the chart differentiate course levels (e.g., beginning, intermediate, and advanced).

B=Beginning, I=Intermediate, A=Advanced, BO=Beginning Optional, IO=Intermediate Optional,
AO=Advanced Optional

2.5 NIST Special Publication 800-16 Mapping

The courses in the IT Security Library were designed to meet the requirements specified by the NIST Special Publication 800-16. The process used to map the courses to the requirements is defined below.

Table 1, titled the "800-16 IT Security Training Matrix" is the starting point for defining effective Role-based training, as it maps out the training cell(s) that must be completed to promote specific career/track progression. Refer to NIST Special Pub 800-16, Chapter 4 for specific information regarding the use and structure of this table.

Table 2, titled "Job Function–Training Cross Reference" identifies specific roles and correlates them with the responsibilities listed in Table 1 by mapping specific Job Functions, Roles and Responsibilities to various titles (e.g., System Administrator, DBA, Users, etc.), and provides the basis for the sample Training Plans included in Part II of this catalog.

Table 3 presents the mapping between the NIST SP 800-16 training cells (requirements) and the IT Security Course Curriculum, and demonstrates the method used to map the IT Security Courses to federal guidance documents.

Table 1. NIST SP 800-16 IT Security Training Matrix

	FUNCTIONAL SPECIALTIES						
	A	B	C	D	E	F	G
Training Areas	Manage	Acquire	Design & Develop	Implement & Operate	Review & Evaluate	Use	Other
1 Laws & Regulations	1A	1B	1C	1D	1E	1F	
2 Security Program							
2.1 Planning	2.1A	2.1B	2.1C	2.1D	2.1E		
2.2 Management	2.2A	2.2B	2.2C	2.2D	2.2E		
3 System Life Cycle Security							
3.1 Initiation	3.1A	3.1B	3.1C		3.1E	3.1F	
3.2 Development	3.2A	3.2B	3.2C	3.2D	3.2E	3.2F	
3.3 Test & Evaluation			3.3C	3.3D	3.3E	3.3F	
3.4 Implementation	3.4A	3.4B	3.4C	3.4D	3.4E	3.5F	
3.5 Operations	3.5A	3.5B	3.5C	3.5D	3.5E	3.5F	
3.6 Termination	3.6A			3.6D	3.6E		
4 Other							

 These areas of the matrix are available for future modifications

This table was then used as the basis for the Job Function - Training Cross Reference Table (Table 2), which uses the specific roles and responsibilities defined by the NIST SP 800-16 to define the specific Job Functions, Roles and Responsibilities associated with the various titles (e.g., System Administrator, DBS, Basic User, ISO, etc.). These tables were then used to define the sample Training Plans (Part II) for each respective Job Function / Role.

Table 2. Job Function–Training Cross Reference

The following job functions correspond to the NIST 800-16 IT Security Training Matrix and are recommended for the job titles below. They are defined in Appendix E of the NIST SP 800-16, but are displayed below, for convenience. If a specific job function (role) has responsibilities beyond those listed in the tables below, Table 1 can be used to define the appropriate cells (e.g., 3.2C, 2.2D, etc.) and Table 3 can be used to identify relevant courses in the IT Security Library.

IT Security Officer/Manager		
All cells in the matrix apply		

Database Administrator		
	3.2D	
	3.3D	
	3.4C	
	3.4D	
	3.5D	
	3.6A	
	3.6D	

Programmer/System Analyst		
1C	3.2C	
1D	3.3C	
	3.3D	
	3.4C	
	3.5C	
	3.6D	

Systems Designer/Developer		
1C	3.1A	3.4C
	3.1B	3.5C
	3.1C	
	3.2A	
	3.2C	
	3.3D	
	3.3C	

Information Resources Manager		
1A	2.1A	3.1A
1C	2.1B	3.1E
1E	2.1C	3.2A
1F	2.1D	3.4A
	2.2A	3.6E
	2.2B	
	2.2D	

Network/Systems Administrator			
1D	2.2D	3.3D	3.5D
		3.3D	3.6D
		3.4C	
		3.4D	
		3.5A	
		3.5C	

IT Program Manager			
1C	2.1A	3.1A	3.5A
	2.2A	3.1C	3.5B
	2.2D	3.2E	3.6A
		3.4A	3.6D
		3.4B	
		3.4C	
		3.4E	

System Owner			
1F	2.1A	3.1A	3.3F
	2.2D	3.1B	3.4A
		3.1C	3.4B
		3.1E	3.4E
		3.1F	3.5A
		3.2A	3.5B
		3.2E	3.6A
		3.3E	

Technical Support Personnel			
1D		3.2D	
		3.4D	
		3.5D	
		3.6D	

Information Resources Management Official			
1A	2.1E	3.3E	
1B	2.2C	3.4A	
	2.2D		
	2.2E		

Table 2. Job Function-Training Cross Reference (Cont'd)

The following job functions correspond to the NIST 800-16 IT Security Training Matrix and are recommended for the job titles below. If individuals with the following job titles have additional job functions, they can identify the functions and find the courses that apply by referencing Tables 1 and 3, respectively.

Systems Operations Personnel		
1D	3.2D	3.6D
	3.3D	
	3.4C	
	3.4D	
	3.5C	
	3.5D	

Data Center Manager		
	3.2	
	3.3	
	3.4	
	3.5	
	3.5	
	3.6	
	3.6	

Users		
1F		3.1F
		3.2F
		3.3F
		3.4F
		3.5F

Chief Information Officer			
1A	2.1C	3.4E	
	2.1D		
	2.1E		
	2.2A		
	2.2C		

Designated Approving Authority (DAA)			
	3.3D		
	3.2E		
	3.3E		
	3.4E		
	3.5E		

Table 3. Course to NIST SP 800-16 Cross Reference

This table maps the courses in the IT Security Training Library directly to the requirements detailed in the NIST SP 800-16 (Table 1), indicated by asterisks

[illegible]

Table 3. Course to NIST SP 800-16 Cross Reference (Cont'd)

IT Security Library Mapping to NIST 800-16			National Institute of Standards and Technology (NIST) Special Publication 800-16 Matrix*																																															
Course No.	Course Title	Level	Cell 1A	Cell 1B	Cell 1C	Cell 1D	Cell 1E	Cell 1F	Cell 2.1A	Cell 2.1B	Cell 2.1C	Cell 2.1D	Cell 2.1E	Cell 2.2A	Cell 2.2B	Cell 2.2C	Cell 2.2D	Cell 2.2E	Cell 3.1A	Cell 3.1B	Cell 3.1C	Cell 3.1E	Cell 3.1F	Cell 3.2A	Cell 3.2B	Cell 3.2C	Cell 3.2D	Cell 3.2E	Cell 3.2F	Cell 3.3C	Cell 3.3D	Cell 3.3E	Cell 3.3F	Cell 3.4A	Cell 3.4B	Cell 3.4C	Cell 3.4D	Cell 3.4E	Cell 3.4F	Cell 3.5A	Cell 3.5B	Cell 3.5C	Cell 3.5D	Cell 3.5E	Cell 3.5F	Cell 3.6A	Cell 3.6D	Cell 3.6E		
99031	Implementing Network Security	Int		*						*										*																		*												
99003	Information Encryption with E-commerce	Int											*							*																														
99067	IT Security Awareness	Beg																		*				*												*			*											
99032	IT Security Awareness	Int								*			*							*			*		*											*		*		*										
99036	Integrating Windows NT and Novell NetWare	Int								*				*						*															*			*												
99027	Introduction to Network Security Planning for Windows 2000	Beg												*						*									*						*															
99041	Intrusion Detection	Adv								*								*		*																														
99066	Java Servlet Security	Adv												*						*									*																					
99063	JavaBeans Security	Adv									*			*			*			*						*		*																						
99037	License and Security for Novell NetWare 5	Int								*										*								*																						
99042	Log Analysis	Adv												*						*							*		*										*											
99023	Managing Network Security	Int																	*										*									*		*		*								
99033	Managing Security for Microsoft Internet Explorer	Beg												*						*							*		*									*												
99034	Managing User Security for Windows NT	Int									*									*							*		*									*		*										
99040	Microsoft Proxy Server Security Features	Int																		*							*		*									*												
99009	Network Security Policy	Int								*								*		*							*		*									*												

Table 3. Course to NIST SP 800-16 Cross Reference (Cont'd)

IT Security Library Mapping to NIST 800-16														
Course No.	Course Title	Level	National Institute of Standards and Technology (NIST) Special Publication 800-16 Matrix*											
99021	Network Vulnerabilities and Prevention	Int												
99055	Overview of E-Commerce Security	Beg												
99006	Overview of Java Security	Int												
99007	Overview of Network Security for Windows 2000	Beg												
99029	Pretty Good Privacy	Int												
99044	Principles of Operating Systems Security	Int												
99022	Recovering Data for Windows 2000	Int												
99039	Remote Access Service for Windows NT	Adv												
99047	Risk Management	Int												
99046	Risks Assessment	Int												
99054	Securing Access to Partners	Adv												
99016	Securing an Automated Information System	Int												
99064	Securing Cisco Routers	Adv												
99057	Securing Communication Channels	Int												
99056	Securing Internet Access with Firewalls	Beg												
99018	Securing Local Area Networks	Int												
			Cell 1A	Cell 1B	Cell 1C	Cell 1D	Cell 1E	Cell 1F	Cell 2A	Cell 2B	Cell 2C	Cell 2D	Cell 2E	Cell 2F
			Cell 3A	Cell 3B	Cell 3C	Cell 3D	Cell 3E	Cell 3F	Cell 4A	Cell 4B	Cell 4C	Cell 4D	Cell 4E	Cell 4F
			Cell 5A	Cell 5B	Cell 5C	Cell 5D	Cell 5E	Cell 5F	Cell 6A	Cell 6B	Cell 6C	Cell 6D	Cell 6E	Cell 6F

Table 3. Course to NIST SP 800-16 Cross Reference (Cont'd)

IT Security Library Mapping to NIST 800-16			National Institute of Standards and Technology (NIST) Special Publication 800-16 Matrix*																																																	
Course No.	Course Title	Level	Cell 1A	Cell 1B	Cell 1C	Cell 1D	Cell 1E	Cell 1F	Cell 2.1A	Cell 2.1B	Cell 2.1C	Cell 2.1D	Cell 2.1E	Cell 2.2A	Cell 2.2B	Cell 2.2C	Cell 2.2D	Cell 2.2E	Cell 3.1A	Cell 3.1B	Cell 3.1C	Cell 3.1E	Cell 3.1F	Cell 3.2A	Cell 3.2B	Cell 3.2C	Cell 3.2D	Cell 3.2E	Cell 3.2F	Cell 3.3C	Cell 3.3D	Cell 3.3E	Cell 3.3F	Cell 3.4A	Cell 3.4B	Cell 3.4C	Cell 3.4D	Cell 3.4E	Cell 3.4F	Cell 3.5A	Cell 3.5B	Cell 3.5C	Cell 3.5D	Cell 3.5E	Cell 3.5F	Cell 3.6A	Cell 3.6D	Cell 3.6E				
99020	Securing Network Access	Int																																																		
99049	Securing Network Resources	Int		*										*							*																						*									
99011	Securing Remote Connectivity	Int														*	*										*	*	*								*	*					*	*								
99043	Security Auditing	Adv										*								*																								*								
99002	Security Firewalls for E-commerce	Beg							*		*																																									
99015	Security over Internet Protocol (IPSec)	Int									*							*										*	*								*	*						*								
99026	Security Strategies: External	Int									*	*			*			*	*		*							*	*						*		*	*						*								
99028	Security Strategies: Internal	Int									*	*			*			*	*			*														*	*	*														
99065	Session Beans: Development and Security	Adv									*	*			*	*	*	*		*	*	*					*	*								*	*	*					*	*								
99048	TCP/IP Security	Adv																										*	*								*	*						*	*							
99062	Transaction Management	Int							*											*		*																														
99010	Trouble Shooting Local Area Networks	Int									*	*			*	*	*	*		*							*	*															*	*								
99008	Understanding Kerberos	Int							*		*									*	*							*	*																							
99045	User Account and File System Security	Int									*									*	*	*					*	*															*	*								
99024	Virus Protection and Recovery	Beg									*																*	*																*	*							
99053	Windows 2000 Security Management	Int									*	*						*	*	*	*																															
99035	Windows NT Networking: Multiple Domains	Adv									*									*	*	*					*	*																								

3.0 Course Descriptions

This section of the catalog provides a detailed description of the courses in the IT Security Library, and includes prerequisites and competency levels, when applicable. The library will continue to evolve; updated and new courses will be added as government, industry and academic feedback dictates. Therefore, please keep in mind that this list, although accurate, may not be complete.

Note: Although the examples and exercises in this IT Security Library are geared toward open, standards-based technologies, some exercises require platform-specific instruction. In these cases, Microsoft's Windows platform will be the default—unless otherwise noted.

Courses in the IT Security Library include:

- Advanced Local Network Security
- Analyzing Network Security Plans
- Authentication and Authorization in E-Commerce
- Certification Authority
- CGI and Encryption
- Designing and Configuring Firewalls
- Designing Local Network Security
- Designing Remote Security Solutions
- Designing WAN Security
- Detecting Hackers
- Distributed Security Planning
- E-Commerce Payments Security
- Encrypting File Systems (EFS)
- Firewall Fundamentals
- Fundamentals of Internet Security
- Identifying Viruses
- Implementing Network Security
- Information Encryption with E-Commerce
- IT Security Awareness (Beginning)
- IT Security Awareness (Intermediate)
- Integrating Windows NT and Novell NetWare
- Introduction to Network Security Planning for Windows 2000
- Intrusion Detection
- Java Servlet Security
- Java Beans Security
- License and Security for Novell NetWare 5
- Log Analysis
- Managing Network Security
- Managing Security for Microsoft Internet Explorer
- Managing User Security for Windows NT
- Microsoft Proxy Server Security Features
- Network Security Policy
- Network Vulnerabilities and Prevention
- Overview of E-Commerce Security
- Overview of Java Security
- Overview of Network Security for Windows 2000
- Pretty Good Privacy
- Principles of Operating Systems Security
- Recovering Data for Windows 2000
- Remote Access Service for Windows NT
- Risk Management
- Risks Assessment
- Securing Access to Partners
- Securing an Automated Information System
- Securing Cisco Routers
- Securing Communication Channels
- Securing Internet Access with Firewalls
- Securing Local Area Networks
- Securing Network Access
- Securing Network Resources
- Securing Remote Connectivity
- Security Auditing
- Security Firewalls for E-Commerce
- Security Over Internet Protocol (IPSec)
- Security Strategies: External
- Security Strategies: Internal
- Session Beans: Development and Security
- TCP/IP Security
- Transaction Management
- Trouble Shooting Local Area Networks
- Understanding Kerberos
- User Account and File System Security
- Virus Protection and Recovery
- Windows 2000 Security Management
- Windows NT Networking: Multiple Domain

3.1 Advanced Local Network Security

Duration: 3 Hours

Level: Advanced

In this course you will learn to design a strategy for protecting network data transmission on a private network from a packet-level impersonation into a specified scenario, evaluate a network data protection strategy used to protect the data transmitted on a private network from packet level impersonation, identify the guidelines for selecting network authentication methods, match network authentication methods with their features, match network data transmission risks with the situations in which they can exist, identify the guidelines that are used to authenticate non-Microsoft clients on a Windows 2000 network, and design an authentication strategy for integrating non-Microsoft clients with Windows 2000 Server in a specified scenario. Other topics include:

- Matching the IPSec encryption algorithms with the guidelines used to select them.
- Matching the IPSec authentication methods with the guidelines used to select them.
- The guidelines that are used to select various IPSec integrity algorithms.
- The network authentication method that is best suited for a specified situation.
- Sequencing the steps performed for setting up a Macintosh client connection with a Windows 2000 server.
- Installing File Server for Macintosh by using Windows 2000 Server.
- Configuring File Server for Macintosh by using Windows 2000 Server.
- Creating a Macintosh-accessible volume by using Windows 2000 Server.
- Setting a password for a Macintosh-accessible volume by using Windows 2000 Server.
- Installing authentication files on a Macintosh client.
- Sequencing the steps performed for setting up a NetWare client connection with a Windows 2000 server.
- Installing Gateway Service for NetWare by using Windows 2000 Server.
- Setting the default tree and context by using Windows 2000 Server.
- Enabling a gateway to NetWare resources by using Windows 2000 Server.
- Activating the gateway to NetWare resources by using Windows 2000 Server.
- Changing the NetWare NDS password by using Windows 2000 Server.
- Setting up a Telnet connection by using Windows 2000 Server.

Prerequisite: "Introduction to Network Security Planning for Windows 2000"

3.2 Analyzing Network Security Plans

Duration: 3 Hours

Level: Intermediate

In this course you will learn to create and analyze a network security plan that is based on business, organizational, and technical factors as well as internal and external users. Other topics include:

- Matching organizational structures with their implications on the network security plan.
- The guidelines for a network security plan at various stages of the service and product life cycle.
- The guidelines for the change management plan to ensure network security.
- Matching various types of IT management structures with their characteristics.
- Identifying the most appropriate security plan for a specified technical scenario.
- Identifying the impact of a change in a security plan on the existing technical environment in a specified situation.

3.3 Authentication and Authorization in E-Commerce

Duration: 1 Hour

Level: Intermediate

In this course you will learn about the role of personal and certificate-based authentication in e-commerce. You will also learn about the different types of authentication techniques available. Other topics include:

- Authentication methods for individuals.
- The role of passwords in authentication processes.
- Identifying types of tokens used in authentication processes.
- The features of biometric systems.
- The functions of single sign-on techniques.
- The different types of digital certificates.
- The steps involved in obtaining a personal certificate.
- The steps involved in obtaining a server certificate.

Prerequisite: "Overview of E-Commerce Security"

3.4 Certification Authority

Duration: 2 Hours

Level: Intermediate

In this course you will learn about the advantages and components of Windows 2000 Public Key Infrastructure (PKI). You will also learn to install a Certification Authority (CA) and send a request for a certificate to the CA. Other topics include:

- Matching the types of CAs with the situations in which they are used.
- Installing a CA by using the Windows Components Wizard.
- Configuring a CA by using the Certification Authority snap-in.
- Renewing a CA by using the Certification Authority snap-in.
- Specifying access permissions to a specific user by using the Certification Authority snap-in.
- Making a backup of a CA by using the Certification Authority snap-in.
- Creating a certificate request based on a specific template by using the Certificates snap-in.
- Issuing an advanced certificate template.
- Renewing a certificate by using the Certificate Renewal Wizard.
- Revoking a certificate by using the Certificates snap-in.
- Identify the steps to detect a problem encountered while accessing a CA.
- Matching the problems encountered while accessing a CA with their solutions.

3.5 CGI and Encryption

Duration: 1 Hour

Level: Intermediate

In this course you will learn about the features of Common Gateway Interface (CGI) and the strategies of CGI security. Other topics include:

- The features of Perl.
- The security risks created by CGI scripts.
- The measures used to minimize CGI security risks.
- The features of a CGIWrap application.
- Matching the SSI tag with its function.
- Performing the steps to view a digital certificate using Netscape Navigator 4.6.

3.6 Designing and Configuring Firewalls

Duration: 1 Hour

Level: Intermediate

In this course you will learn to identify the guidelines for designing a firewall for a specific network and the appropriate firewall design based on the security requirements of a specific network. Other topics include:

- Configuring WinRoute to segregate internal and external networks.
- Creating packet filters to prevent the transfer of packets of specific types from one network to another.

Prerequisites: "Firewall Fundamentals", "Securing Internet Access with Firewalls" and "Security Firewalls for E-Commerce"

3.7 Designing Local Network Security

Duration: 4 Hours

Level: Advanced

In this Windows 2000-centric course, you will learn to evaluate the permission set applied for files and folders for the specified requirements, match standard folder, file and special access permissions with their descriptions, identify the rules that control access permissions for files and folders, identify the appropriate access design for specific files and folders, match different types of backup with their functions, identify guidelines to create a backup plan, and identify the decisions involved in planning an audit policy for a specified situation. Other topics include:

- Matching printer permissions with their descriptions.
- Matching the types of printer users with their descriptions.
- Matching printer configuration options with their uses.
- The considerations for ensuring printer security in an organization.
- Designing a strategy to ensure printer security in a specified situation.
- Evaluating printer security in a specified scenario.
- The characteristics of EFS.
- Identifying the recovery policy considerations for implementing EFS in an organization.
- Identifying the considerations for implementing EFS in an organization.
- Designing an EFS strategy in a specified situation.
- Matching the types of security templates with their uses.
- Identifying the security settings for a kiosk.
- Identifying the security settings for a portable computer.
- Matching the events that can be audited in Windows 2000 with their descriptions.
- Identifying the considerations to secure Windows 2000 DNS.
- Designing security for a Windows 2000 DNS server.
- Matching RIS security strategies with the situations in which they are used.
- Setting SNMP security properties by using the Computer Management console.

3.8 Designing Remote Security Solutions

Duration: 2 Hours

Level: Intermediate

In this course you will learn about the features of CA, how to match the CA types with the functions that they perform, guidelines for implementing a specific hierarchy of CAs to secure remote access, guidelines to be followed for integrating a third-party CAs with their purposes. Other topics include:

- PKI encryption method to be used in a specified situation.
- The features of a certificate server.
- Matching the certificate management processes with the situations in which they are used.
- Identifying the situation in which a specific type of certificate mapping is used.
- Implementing the appropriate certificate management process in a specified situation.
- Designing strategies in a PKI to provide security to the network of an organization.

3.9 Designing WAN Security

Duration: 2 Hours

Level: Intermediate

The Designing WAN Security course will teach you the principles of WAN security and strategy, identify the most appropriate design implementation decisions to provide secure remote access to an enterprise network, to match the remote access policy elements with the scenarios in which they are used, and how to design a Windows-based remote access security strategy. Other topics include:

- Matching the various types of firewalls with their basic functions.
- Identifying the functions of the Proxy server.
- The benefits of RADIUS.
- The benefits of demand-dial routing.
- The benefits of a VPN.
- Identifying the most appropriate RAS security element to be used in a specified situation.
- Matching RAS authentication protocols with the situations in which they are used.
- Identifying the situations in which the use of a specific RAS encryption method is appropriate for securing data.

Prerequisite: "Firewall Fundamentals"

3.10 Detecting Hackers

Duration: 1 Hour

Level: Intermediate

In this course you will learn to identify the response plan to be executed on the basis of the scope of security breach in the event of a hacker attack and to identify the appropriate strategy to respond to a hacker in a specific situation. Other topics include:

- Matching the proactive detection techniques with the corresponding situations to ensure security on a network.
- Creating a dummy account to distract a hacker by using User Manager for Domains.
- Identifying the correct block of commands to install the Tripwire program.

3.11 Distributed Security Planning

Duration: 2 Hours

Level: Intermediate

In this course you will learn to design strategies for assigning memberships to Windows 2000 security groups and planning the delegation of administration. In addition, you will learn about placing and inheriting security policies in sites, domains and OUs. Other topics include:

- Matching various types of security groups with their scopes.
- Identifying the default access rights granted to built-in Windows 2000 administrative groups.
- Considerations for assigning memberships to security groups.
- Matching security group scopes with the situations in which they are used.
- Designing a security group strategy for easy administration and enhanced network performance.
- Designing a strategy to delegate administrative authority.
- Identifying the recommendations for designing Group Policy.

3.12 E-Commerce Payments Security

Duration: 1 Hour

Level: Intermediate

In this course you will learn about electronic cash, smart cards, credit and debit cards. Other topics include:

- The features of SET.
- The features of the iKP protocols.

Prerequisite: "Overview of E-Commerce Security"

3.13 Encrypting File System (EFS)

Duration: 1 Hour

Level: Intermediate

The Encrypting File System (EFS) course covers the uses of Windows 2000 EFS and the procedures for encrypting a file. Other topics include:

- Encrypting a file by using the Advanced Attributes dialog box.
- Adding a recovery agent to Group Policy by using the Add Recovery Agents Wizard.
- Deleting a recovery agent from the local computer by using the Group Policy snap-in.

3.14 Firewall Fundamentals

Duration: 1 Hour

Level: Beginning

In this course you will learn basic firewall design principles, identify the roles of firewalls and their types, learn about the packet-filtering rules used to implement a security policy, and match the various firewall types with the situations in which they are best deployed. Other topics include:

- The packet-filtering rule used to implement a security policy.
- Matching the types of proxy servers with the scenarios in which they are used.
- Installing Proxy Server on a network by using Microsoft Proxy Server 2.0 CD.
- Enabling access control for Web proxy service on a proxy server by using MMC.
- Setting up RAS to use a VPN connection on a Windows NT server.
- Establishing a VPN session by using RAS.

3.15 Fundamentals of Internet Security

Duration: 3 Hours

Level: Intermediate

In this course you will learn to match the data security features with the situations in which they are used, identify the security requirements for a network in a specified situation, match the data encryption methods with the situations in which they are used, match the encryption standards with the situations in which they are applicable, match the types of authentication with the situations in which they are used, and match the elements of an authentication certificate with their functions. Other topics include:

- Identifying the network resources whose user-access levels are controlled by an ACL.
- Matching the type of filtering used by a screening router with the situation in which it is used.
- Matching the functions performed by a proxy server with the situations in which they are applicable.
- Matching the types of CAs with the situations in which they are used.
- Matching the network activities to be audited with the specified auditing requirements.
- Matching the types of logs with the situations in which they are used.
- Identifying the activities detected by IDS utilities.
- Matching the virus types with the damages caused by them.
- Sequencing the steps for deploying an anti-virus program on a computer.
- Matching the types of suspicious activities with the situations where they occur.
- The features of a VPN.
- The type of VPN used in a specified situation.
- Matching the VPN protocols with the situations where they are used.
- Establishing a VPN connection to a site by using the My Computer icon in Windows 98.

Prerequisite: "Securing Internet Access with Firewalls"

3.16 Identifying Viruses

Duration: 2 Hours

Level: Beginning

In this course you will learn about the characteristics of viruses and malicious programs. You will also learn to identify the methods that are used by retroviruses to interfere with the operation of anti-virus programs. Other topics include:

- Matching a virus type with the method used to conceal it.
- The statements that describe a traditional virus.
- The statements that describe a boot sector virus.
- The statements that describe a macro virus.
- Selecting the operations of a polymorphic virus.
- The operations of a stealth virus.
- The operations of a slow virus.

3.17 Implementing Network Security

Duration: 2 Hours

Level: Intermediate

This course covers the safeguards that prevent, detect and correct physical access threats to the network and help establish employee accountability for physical LAN access. Other topics include:

- Electronic network threat detection safeguards.
- Matching the management control safeguards that prevent threats to LANs with their roles.
- Matching the management control safeguards for detecting threats to LANs with their roles.
- Management control safeguards that help in containing threats.

Prerequisites: "Overview of Network Security for Windows 2000", "Introduction to Network Security Planning for Windows 2000", "Implementing Network Security", and "Network Security Policy"

3.18 Information Encryption with E-Commerce

Duration: 2 Hours

Level: Intermediate

In this course you will study an overview of information encryption. You will also examine different encryption techniques and encryption services. Specific topics include:

- The forms of attack that data encryption protects against.
- The characteristics of public and secret key encryption systems.
- The role of global legislation in monitoring encryption techniques.
- The features of Data Encryption Standard (DES).
- The features of the Pretty Good Privacy (PGP) encryption method.
- The features of the RSA encryption method.
- The public key cryptography standards (PKCS).
- The features of the Kerberos model.
- The components of a public key infrastructure (PKI).
- The features of Secure Sockets Layer (SSL).
- The features of the IPSec protocol.
- The technologies that allow for secure electronic mail.
- The role of a Virtual Private Network (VPN) in e-commerce.

Prerequisites: "Overview of E-Commerce Security for Windows 2000", "Pretty Good Privacy", and "Understanding Kerberos"

3.19 IT Security Awareness (Beginning) *NEW COURSE*

Duration: .5 Hours

Level: Beginning

In this course, you will learn why computer security is important and what you can do to help reduce threats to security. You will learn about issues such as laws and government regulations, threats, vulnerabilities, email security, social engineering, and individual accountability. Other topics include:

- Roles and responsibilities in IT security
- Ways to protect shared data
- Examples of internal and external threats
- Viruses and worms
- Security controls such as passwords
- Ways to recognize an IT security incident

3.20 IT Security Awareness (Intermediate)

Duration: 1 Hour

Level: Intermediate

In this course, you will learn why computer security is important and what you can do to help reduce threats to security. You will also learn about current issues such as threats, vulnerabilities, and countermeasures; contingency planning; protection of data and software from unauthorized access; and laws and government regulations. Other topics include:

- Categories of Threats – intentional, unintentional, and natural
- Examples of IT Security Threats, including insider threats and social engineering
- Impacts of threats on IT resources
- Individual accountability
- Destruction, modification, disclosure, denial of service
- Viruses

3.21 Integrating Windows NT and NetWare

Duration: 1 Hour

Level: Intermediate

The Integrating Windows NT and NetWare course will teach you the benefits of integrating Windows NT domains with NDS as well as the management capabilities of NDS. Other topics include:

- Installing NDS for NT by using the installation CD-ROM.
- The appropriate user action that should be applied to users in a group when migrating to NDS in a given scenario.
- Migrating the objects in a Windows NT domain to an NDS tree by using the Domain Object Wizard.
- The guidelines for placing an NDS replica in an integrated environment.
- Placing an NDS replica on a Windows NT server by using the Domain Object Wizard.

3.22 Introduction to Network Security Planning for Windows 2000

Duration: 2 Hours

Level: Beginning

In this course you will learn to identify the components of the Windows 2000 security model with their functions and match the Windows 2000 encryption technologies with the situation in which they provide security. Other topics include:

- Matching various disclosures of data attacks with their descriptions.
- Matching various corruptions of data threats with their descriptions.
- Matching the various denials of service attacks with their descriptions.
- Identifying the potential threats against which the most important resources are to be secured.
- Matching the features of Windows 2000 Active Directory with the threats against which they protect a network in a specified situation.
- Matching the authentication protocols with the situations in which they are used.
- Matching the Windows 2000 access control features with the situations in which they provide security.

3.23 Intrusion Detection

Duration: 3 Hours

Level: Advanced

In this course you will learn to identify the advantages of using an IDS in a specified scenario and identify the appropriate IDS architecture for a network in the specified situation. Other topics include:

- Conducting a security scan by using eTrust Intrusion Detection.
- Conducting a network activity trace by using the eTrust Intrusion Detection window.
- Creating an intrusion detection rule by using the Intrusion Attempt Detection Rules dialog box.
- Installing ITA on a Windows NT system by using the Intruder Alert wizard.
- Connecting to an ITA manager by using ITA Admin.
- Activating the required policies for a domain by using the shortcut menu in the Intruder Alert 3.0 window.
- Scanning specific activities by using ITA View.
- Registering an agent with additional managers by using ITA Setup.

3.24 Java Servlet Security

Duration: 1 Hour

Level: Advanced

In the Java Servlet Security course you will learn to complete the code used in basic authentication, the code used in digest authentication and SSL authentication. Other topics include:

- Creating an ACL for a user.
- Creating an ACL for a group of users.

3.25 JavaBeans Security

Duration: 3 Hours

Level: Advanced

Match security threats with the situations in which they occur in an enterprise environment, match security identities with their features, match the security attributes that are set in the deployment descriptor with their functions, complete the code that is used to provide programmatic security logic to an enterprise application, complete the security declaration of a specified role in the deployment descriptor of an enterprise application, and identify the situations in which secure authentication should be implemented in an enterprise environment. Other topics include:

- Completing the security declaration of a specified method permission in the deployment descriptor of an enterprise application.
- Matching the entries in a deployment descriptor to declare method-driven authorization with the situations in which they are used.
- Identifying the communication channel that is used in a specified situation.
- Identifying the security-related services provided by the Enterprise Bean Provider.
- Identifying the security-related services provided by an Application Assembler.
- Identifying the security-related services provided by the Deployer.
- Identifying the situations in which RMI should be implemented in an enterprise environment.
- Matching RMI architectural entities with their functions.
- The uses of object serialization.
- The guidelines that are followed when implementing object serialization.
- The guidelines for passing parameters by using Java RMI.
- The underlying logic of the displayed piece of code that performs a step in RMI implementation.
- Matching the security functions of an EJB container with the way in which they are implemented.
- Matching security APIs with their functions.
- Identifying the situations in which it is advantageous to merge RMI with CORBA.
- Sequencing the steps that are performed to merge RMI with CORBA.
- Matching the problems that arise when merging RMI and CORBA with their solutions.

3.26 Licensing and Security for Novell NetWare 5

Duration: 2 Hours

Level: Intermediate

In this course you will learn to identify characteristics of license objects, interpret license information of a NetWare 5 server, access the appropriate option for a given user account restriction task, and set restrictions on a user account by using the password properties. Other topics include:

- Assigning license units to users in a NetWare network by using NetWare Administrator.
- Installing additional licenses for users in the NDS tree by using NetWare administrator.
- The different types of network security provided by NetWare 5.
- Completing a flowchart of the login process in a NetWare 5 network.
- Establishing intruder detection for users in a container by using NetWare Administrator.
- The guarantees of the authentication process provided by NetWare 5 login security.

3.27 Log Analysis

Duration: 1 Hour

Level: Advanced

In this course you will learn to match the specified situation with the Windows NT logs that can provide information about the situation, enable directory auditing in Windows NT, and filter logs in Windows NT to display specific events. Other topics include:

- Displaying Debug Log on a firewall by using WinRoute.
- Identifying the information that a specific entry in the Debug Log represents.
- The correct Linux command to filter a Linux log.

3.28 Managing Network Security

Duration: 2 Hours

Level: Intermediate

The Managing Network Security course will cover procedures for creating and configuring system services and security options in Windows 2000. In addition, you will learn to configure password policy settings, account lockout policy settings, audit policy settings and user rights assignments. Other topics include:

- Adding the Security Templates snap-in to the MMC console by using the Run dialog box.
- Creating a security template by using the Security Templates snap-in.
- Adding the Security Configuration and Analysis snap-in to the MMC console.
- Setting up a security database by using the Security Configuration and Analysis snap-in.
- Analyzing security configuration by using the Security Configuration and Analysis snap-in.
- Applying security settings to a domain by importing a security template into a Group Policy object.
- Identifying the solution for a specific Local policy problem.

Prerequisites: "Overview of Network Security for Windows 2000", "Introduction to Network Security Planning for Windows 2000", "Implementing Network Security", and "Network Security Policy"

3.29 Managing Security for Microsoft Internet Explorer

Duration: 2 Hours

Level: Beginning

In this course you will learn to identify the types of security zones and set-up a site for a local intranet zone as well as identifying the uses of certificate servers and digital certificates and learn to configure a certificate. Other topics include:

- ActiveX controls and plug-ins security options.
- Java security options.
- Scripting security options.
- User Authentication security options.
- Miscellaneous security options.
- Identifying the issues to be considered when choosing a Certificate Authority.
- Configuring the Java security options.
- Adding the rating system file to the Content Advisor.

3.30 Managing User Security for Windows NT

Duration: 2 Hours

Level: Intermediate

In this course you will learn to identify the Windows NT features that are used to control user access to resources and match the methods that are used for implementing security in Windows NT and their functions. Other topics include:

- Creating an account policy for all the accounts in a domain by using User Manager for Domains.
- Setting a user rights policy for a user account by using User Manager for Domains.
- Creating an audit policy for a domain by using User Manager for Domains.
- The features of the types of user profiles.
- Modifying a local user profile by using Control Panel.
- Creating a roaming user profile by using User Manager for Domains.
- Creating a default roaming user profile by using User Manager for Domains.
- Creating a mandatory user profile by using the Windows NT Explorer.
- The functions of a system policy.
- Setting a system policy for a user by using the System Policy Editor.

Prerequisite: "Principles of Operating System Security"

3.31 Microsoft Proxy Server Security Features

Duration: 2 Hours

Level: Intermediate

In the Microsoft Proxy Server Security Features course you will learn about the guidelines for setting Windows NT security parameters for Proxy Server and learn how to configure server authentication and Web Proxy domain filter permissions by using the Microsoft Management Console Window. Other topics include:

- Disabling IP forwarding.
- The methods of protecting LAN from the Internet.
- Granting permissions to users for accessing Internet services by using the Microsoft Management Console window.
- Configuring Proxy Server for use with WinSock applications.
- Identifying the information contained in the packet type parameters.
- The benefits of packet filtering.
- Creating a packet filter by using the Microsoft Management Console window.
- Matching the packet log record information with their respective log fields.
- Identifying the events for which alerts should be generated.
- Configuring event alerts on the Web Proxy service.
- Configuring alerts as an e-mail message.

3.32 Network Security Policy

Duration: 1 Hour

Level: Intermediate

This course will present the factors that influence the security policy of a network and you will learn to identify the guidelines for creating a secure password and user account policy. Other topics include:

- Identifying the security model that is used for a specific network.
- Identifying the encryption scheme used to encrypt data in a specific scenario.
- Identifying the situation in which digital signatures are used.
- The type of filtering used by a screening router to filter data packets in a specific scenario.
- The functions of a proxy server.

Prerequisite: "Analyzing Network Security Plans"

3.33 Network Vulnerabilities and Prevention

Duration: 2 Hours

Level: Intermediate

This course covers information about the general network security threats and the tools for reducing network and database security threats. You will also learn to identify system and personnel policies for reducing security threats, different types of anti-virus software, and functions of virus scanners, integrity checkers and behavior blocker anti-virus programs. Other topics include:

- Identifying the reasons for LANs vulnerability to security threats.
- The different types of computer viruses.
- The damages caused by a virus to a system.
- The functioning of boot sector and file viruses.
- The features of polymorphic and stealth viruses.
- The types of computer malware.

Prerequisites: "Firewall Fundamentals", "Identifying Viruses", and "Virus Protection and Recovery"

3.34 Overview of E-Commerce Security

Duration: 1 Hour

Level: Beginning

In the Overview of E-Commerce Security course you will learn to identify strategies for minimizing the risks involved in e-commerce and the steps for securing an E-Commerce Web server. Other topics include:

- The features of SSL.
- The features of SET.
- The strategies used that help to recover from a security breach.

3.35 Overview of Java Security

Duration: 1 Hour

Level: Intermediate

In this course, you will learn about the features of Java and the different types of security risks associated with Java. In addition, you will learn to identify the functions of a Class Loader and Security Manager. Other topics include:

- The functions of Bytecode Verifier.
- The security options in Java Applet Viewer.
- Performing the steps to set Java in Netscape Communicator 4.6.

3.36 Overview of Network Security for Windows 2000

Duration: 1 Hour

Level: Beginning

This course will cover the network security features of Windows 2000. You will learn to match the tools used for securing a Windows 2000 network with the situation in which they are used. Other topics include:

- Matching the components of the Security Configuration Tool Set with their functions.
- Identifying the Security Configuration policy that provides security for a specific function.

3.37 Pretty Good Privacy

Duration: 2 Hours

Level: Intermediate

In this course you will learn about the functions and vulnerabilities of Pretty Good Privacy (PGP). You will also about advanced PGP operations and will be able to identify the benefits of modifying a PGP configuration file. Other topics include:

- Matching the PGP version with its description.
- Matching the key management command with its use.
- Performing the steps to generate a PGP key pair using DOS commands.
- Encrypting an e-mail message using PGP.
- Matching a PGP configuration file variable with its use.

3.38 Principles of Operating Systems Security

Duration: 1 Hour

Level: Intermediate

This course will cover the different security services and components that should be used in a specified situation, the resources that requires a particular level of security and the security mechanism that should be implemented to meet the requirements in the specified scenario. Other topics include:

- Matching EALs of CC with the scenarios in which they are applicable.
- Completing the diagram to depict the user authentication process that involves Windows NT security subsystem components.

3.39 Recovering Data for Windows 2000

Duration: 2 Hours

Level: Intermediate

This course will cover the methods used to recover a Windows 2000 network and a Windows 2000 server from a specific problem. You will learn to match the method used to start a failed server with the problem that prevents the server from starting as well as sequencing the steps to recover a server in the safe mode. Other topics include:

- Installing the Recovery Console by using the Windows 2000 CD-ROM.
- Identifying the repair tasks performed by the Recovery Console to start Windows 2000.
- Repairing a Windows 2000 server by using the Recovery Console commands.
- Sequencing the tasks to be performed for rebuilding a Windows 2000 server.
- Restoring Active Directory by restoring the System State data.
- Performing authoritative restore for the Organizational Unit (OU) that contains Active Directory objects by using ntdsutil.exe.

Prerequisites: "Introduction to Network Security Planning for Windows 2000" and "Overview of Network Security for Windows 2000"

3.40 Remote Access Service for Window NT

Duration: 2 Hours

Level: Advance

In the Remote Access Service for Windows NT class you will learn to install Remote Access Service (RAS) through the network program item of the Control Panel and learn to install the software. You will also learn to configure RAS with TCP/IP and the IPX protocol and it will teach you how to configure encryption to ensure RAS security: data encryption and password encryption. Other topics include:

- Configuring the RAS server to support the NetBEUI protocol.
- Creating the DEVICE.LOG file to aid troubleshooting a modem problem.
- Creating the PPP.LOG file to aid troubleshooting PPP authentication problems.
- The features of TAPI and configuring a TAPI location.
- Configuring RAS Permissions to ensure the validity of the user accessing the RAS server: Grant dial-in permissions. Revoking dial-in permissions.
- Configuring the RAS server for callback security options using the Remote Access Admin tool: Preset To. Setting By Caller. No Callback.

3.41 Risk Management

Duration: 2 Hours

Level: Intermediate

This course will cover registry access permissions to be set in a specified situation and implementing an audit policy by using Windows NT's User Manager for Domains. You will also learn to identify the md5sum command that will be used in a specified situation. Other topics include:

- Removing a subsystem from a Windows NT system by using the C2 Configuration command.
- Identifying the steps to control SMB connectivity on a Windows NT server.
- Disabling the Server service by using the Services icon.
- Identifying the option that disables the Telnet service.
- Applying system patches by installing Service Pack 6a.
- Securing the Windows NT registry by using the C2 Configuration command.
- Identifying the tasks to enable the TCPWrapper suite on a UNIX platform.

3.42 Risks Assessment

Duration: 1 Hour

Level: Intermediate

This course will present various types of security attacks on Windows NT-based systems and the situations in which they have occurred. You will learn to identify the situations in which the NFS should be used and match the NIS security problems with the appropriate solutions. Other topics include:

- Installing a KeyLogger program by using the iksnt10d.exe file.
- Disabling Windows NT default shares by using the Regedit command.
- Scanning a Windows NT system by using the WS_Ping ProPack program.
- Identifying the command to log on to a remote computer.

3.43 Securing Access to Partners

Duration: 2 Hours

Level: Advanced

In this course you will learn to identify the features of Windows NT/2000's user account-based authentication method, the trusted domain-based authentication method, and certificate-based authentication method. It will also cover the guidelines for selecting an appropriate authentication method and the appropriate strategy for authenticating trusted partners. Other topics include:

- Matching the placement of a VPN server in conjunction to a firewall with its related benefits.
- Evaluating the effectiveness of a VPN solution for a given scenario.
- The benefits of Terminal Services.
- The security features of Terminal Services.
- The features of message queuing.
- Sequencing the steps involved in message queuing authentication.

3.44 Securing an Automated Information System

Duration: 2 Hours

Level: Intermediate

In this course you will learn to identify the components of a security analysis of the network, strategies used to counter risks to the network system, identify risks to the system security and various strategies to protect a system such as access control, authentication, passwords, encryption, biometrics, modem security, and firewalls. Other topics include:

- Matching methods of authenticating users with their functions: authentication by possession, authentication by intrinsic characteristics, and authentication by knowledge.
- Describing guidelines for choosing effective passwords.
- Matching biometric analyses with their function: fingerprint analysis, handprint analysis, voice pattern analysis, handwriting analysis, keystroke analysis, and retina scans.
- Ways of preventing illegal access to a network through modem dial-ups.
- Various techniques used to disguise data in order to protect it from unauthorized users.
- The features of the public/private key encryption technique.
- Sequencing the steps involved in the Kerberos authentication process.
- The features of Pretty Good Privacy.
- Matching the methods of masking data with their functions: electronic signature, clipper, compression, padding, and lost in a crowd.

3.45 Securing Cisco Routers

Duration: 3 Hours

Level: Advanced

In this course you will learn to identify the situations in which Network Address Translation (NAT) implementation is useful, identify the functions of Port Address Translation (PAT), identify the advantages and disadvantages of NAT implementation, perform the steps to configure static NAT for inside local translations on a Cisco router, perform the steps to configure dynamic NAT for inside local translations on a Cisco router, and perform the steps to configure NAT for inside global address overloading on a Cisco router. Other topics include:

- The steps to configure NAT for TCP load distribution on a Cisco router.
- Configuring NAT for TCP load distribution on a Cisco router.
- Configure NAT for overlapping address translation on a Cisco router.
- Configure PAT on a Cisco 700 router.
- Associating each application with its corresponding Cisco security solution.
- CiscoSecure ACS features.
- Matching the AAA elements with their definitions.
- Enabling CiscoSecure ACS access and AAA services on a NAS.
- Configuring AAA authentication for client access control on a NAS.
- Configuring AAA authorization for client access control on a NAS.
- Configuring AAA accounting for client access control on a NAS.
- Sequencing the steps of virtual profile operation.

3.46 Securing Communication Channels

Duration: 2.2 Hours

Level: Intermediate

In this course you will learn to identify the features of IPSec communication modes, match the IPSec protocols with their features, match predefined security policies with their features, match the activities that occur in an IPSec management strategy with their examples, identify the actions that need to be performed while designing an IPSec policy, identify the sequence of steps in the phases of IPSec negotiation, and identify the situation in which you use a specific security level. Other topics include:

- Matching the data authentication methods with the situations in which they are to be used.
- Matching the algorithm with the guidelines for selecting the algorithm.
- Matching the filter action with the guidelines for selecting the filter action.
- Designing an IPSec solution in a specified scenario.
- Analyzing an IPSec design in a specific situation.
- The features of SMB.
- Enabling SMB signing by using the registry editor.
- The features of CIFS.

Prerequisite: "Securing Over Internet Protocol (IPSec)"

3.47 Securing Internet Access with Firewalls

Duration: 1 Hour

Level: Beginning

In this course you will learn to identify the security threats introduced by Internet connections, the benefits and limitations of a firewall, the different components of a firewall and their functions as well as identifying guidelines for selecting a firewall implementation for a specified situation. Other topics include:

- Matching the various types of firewall implementations with their security features.
- Identifying the appropriate server placement strategy to be used in a given situation.
- Evaluating a firewall strategy in a specific situation.

3.48 Securing Local Area Networks

Duration: 2 Hours

Level: Intermediate

In this course you will learn about the backup strategy that is to be implemented in the specified scenario, requirements of a user for making backups on a network, factors to be considered while planning for a disaster and data recovery options. Other topics include:

- Labeling a scenario with the virus type that is causing problems in the specified scenario.
- Identifying the tasks to be performed to prevent a virus infection.
- Identifying the benefits that are derived from a UPS in a specified scenario.
- Labeling a scenario with the type of UPS that is to be used in the specified scenario.
- Matching each level of Redundant Array of Independent Disks (RAID) with the strategy used in the level.
- Labeling each RAID level with its advantage.
- Identifying the RAID level to be selected in a specified scenario.

Prerequisites: "Firewall Fundamentals", "Pretty Good Privacy", and "Understanding Kerberos"

3.49 Securing Network Access

Duration: 2 Hours

Level: Intermediate

In the Securing Network Access course you will learn about the various tools used to provide network access security, such as identifying the benefits of a firewall, matching the firewall mechanism with the security services it provides, and identifying the questions that help establish a firewall design policy. Other topics include:

- Matching the security item with the element of authentication of which it is representative.
- Matching the authentication protocol with the statement that describes it.
- The benefits of a proxy server.
- Matching the type of proxy server deployment with its definition.
- Matching the firewall architecture containing a proxy server with its definition.
- Sequencing the equations that are used to estimate server load.
- Variables to consider when hardware sizing for Netscape Proxy Server 3.5.
- Identifying the services to configure when deploying Netscape Proxy Server 3.5.
- Identifying the configuration issues to consider when implementing a proxy server.
- Identifying the areas of proxy server performance that should be regularly monitored.

Prerequisites: "Firewall Fundamentals", "Microsoft Proxy Server Security Features" and "Security Internet Access with Firewalls"

3.50 Securing Network Resources

Duration: 2 Hours

Level: Intermediate

In this course you will learn to identify the strategies that comply with the guidelines of a security implementation model in a specific situation, identify the guidelines that should be followed to secure services and a Web server in a specific situation, identify the strategies that conform to the guidelines for ensuring network security and the uses of a specific tool that is used to test network security. Other topics include:

- Strategies used to prevent security holes in CGI scripts in a specific situation.
- Securing a Web server by using MMC.
- Identifying the situation that conforms to the guidelines for securing an FTP server.
- Securing an FTP server by using MMC.
- Identifying a scenario where the guidelines for securing an SMTP server are followed.
- Matching the security options that you configure to secure an SMTP server with their functions.

Prerequisites: "Introduction to Network Security Planning" and "Overview of Network Security for Windows 2000"

3.51 Securing Remote Connectivity

Duration: 3 Hours

Level: Intermediate

In this course you will learn to identify the networking functions provided by an effective remote access implementation, identify the limitations of remote access connections, identify the physical location where the remote access server is installed in a specific scenario, identify the services to be provided to remote users in a specific scenario, identify the factors that determine the design of an organizational security policy, identify the factors to be considered while designing the security policy of a network. Other topics include:

- The features of POTS.
- The features of ISDN.
- The features of xDSL.
- Matching the data transmission technologies with the situations in which they are used.
- Identifying the factors that determine the design of a data-level security policy.
- Identifying the advantage of isolating the remote access server.
- Identifying the tasks that optimize the performance of a remote client.
- Identifying the tasks that improve remote server performance.
- Identifying the modem configuration parameters that must be set for a remote connection.
- Configuring a Windows 98 client for remote access.
- Connecting a Windows 98 client remotely to a server by using a specific remote connection.
- Configuring a Windows NT client for remote access.
- Connecting a Windows NT client remotely to a server by using a specific remote connection.

3.52 Security Auditing

Duration: 1 Hour

Level: Advanced

In this course you will learn to match auditing categories with the recommendation that can be made in each category for enhancing security, identify the most appropriate audit report format and identify a host auditing solution for a specified problem. Other topics include:

- Methods for securing a router from forwarding a DOS attack in a specified situation.
- Detecting whether or not the NIC of a computer is in promiscuous mode by using AntiSniff.
- Installing the ConSeal PC FIREWALL service by using the Network dialog box.
- Sequencing the steps to install SSH on a Linux computer.
- Steps for establishing a user-to-user trust relationship in Linux.

3.53 Security Firewalls for E-Commerce

Duration: 2 Hours

Level: Beginning

In this course you will learn about the role of a security policy in e-commerce, approaches to security risk assessment, features of a firewall, the different levels of firewall implementation, and the role of personal firewalls in e-commerce. Other topics include:

- The features of network security relating to access administration.
- Physical security options.
- The risks involved in downloading code via a Web browser.
- The features and functions of packet-filter firewalls.
- The features and functions of proxy firewalls.
- The features of dynamic firewalls.

3.54 Security Over Internet Protocol (IPSec)

Duration: 2 Hours

Level: Intermediate

In this course you will learn to identify the benefits of IPSec, the functions of IPSec protocols, identify a situation in which a (Windows 2000-based) IPSec configuration mode will be used, identify the steps to detect a problem encountered while using IPSec, and match the problem encountered while using IPSec with their solutions. Other topics include:

- Enabling IPSec by using the Internet Protocol (TCP/IP) Properties dialog box.
- Configuring an IPSec policy by using the Add/Remove Snap-in command.
- Creating an IPSec policy by using the IP Security Policy Wizard.
- Adding an IPSec rule to an IPSec policy by using the Security Rule Wizard.
- Identifying the tab that is used to edit the property of an IPSec rule in a specified situation.
- Managing an IPSec policy by using the Action menu.
- Adding an IP filter list to an IPSec rule by using the IP Filter Wizard.
- Editing an IP filter list by using the Manage IP filter lists and filter actions dialog box.
- Adding a filter action to an IPSec rule by using the Filter Action Wizard.
- Editing a filter action by using the Manage IP filter lists and filter actions dialog box.
- Monitoring IPSec statistics by using the ipsecmon command.

3.55 Security Strategies: External

Duration: 2 Hours

Level: Intermediate

In this course you will learn to identify the safeguards used to protect against UNC threats, source routing threats, threats to service, threats to shares, threats to the Anonymous account, SYN threat, and software tools that pose potential threats to a Windows NT/2000-based system. Other topics include:

- Identifying the signs of intruder activity on a network.
- Establishing an audit trail on a directory using File Manager in Windows NT.
- Establishing an audit trail based on an audit policy using the User Manager in Windows NT.
- Setting the event Viewer to display events occurring during a particular time period.
- The uses of sniffing.
- Matching the sniffing prevention tactic with the network scenario.
- Spoofing methods.
- Matching the spoofing prevention tactic with its spoofing method.

Prerequisite: "Network Vulnerabilities and Prevention"

3.56 Security Strategies: Internal

Duration: 1 Hour

Level: Intermediate

In this course you will learn to match the physical access barrier with the security risk it prevents, match the tactic that prevents an electronic threat to a network with its security function, select the tactics for detecting electronic threats to an electronic network, and identify the attributes of a network recovery plan. Other topics include:

- Matching the management safeguard for a LAN with its function.
- Safeguards that establish employee accountability for physical access to a LAN.

Prerequisites: "Network Vulnerabilities and Prevention", and "Securing Local Area Networks"

3.57 Session Beans: Development and Security

Duration: 2 Hours

Level: Advanced

In this course you will learn to match the components of a session bean with their functions, match the Session Bean interface methods with the associated events in the session bean life cycle, complete the code to manage a handle to a session bean from a client application, select the appropriate security policy for EJBs to be deployed based on the specifications of an enterprise network, declare bean authorization requirements in the deployment descriptor of a bean, and complete the code to implement the specific authorization requirements of a session bean. Other topics include:

- Completing the code to create the bean class for a stateful session bean.
- Completing the code to maintain the state of a stateful session bean.
- Completing the code that removes a stateful session bean from an EJB container.
- Completing the code to create the remote interface for a specified stateful session bean.
- Completing the code to create the home interface for a specified stateful session bean.
- Completing the code to create a deployment descriptor to deploy a stateful session bean by using XML.
- Deploying a bean in an enterprise network by using IBM WebSphere 3.5.
- Completing the code to call the methods of a stateful session bean from a Java client application.
- Matching each method of the Session Context interface with the situation in which it is used.
- Selecting the appropriate pool settings to ensure the optimum swapping of stateless session beans by the bean container.

3.58 TCP/IP Security

Duration: 1 Hour

Level: Advanced

In the TCP/IP Security course you will learn to match the methods to breach security in the lower-level OSI layers with the specific situation and to match the methods to breach network security in the application layer of the OSI model with the corresponding situations. Other topics include:

- Configuring Windows NT Server to lock a specific port by using the TCP/IP Security dialog box.
- Conducting a traceback to a Windows NT server from a Linux computer by using plisten.
- Identifying the correct set of commands to establish a connection to a port of a Windows NT server from another computer by using Netcat.

3.59 Transaction Management

Duration: 2 Hours

Level: Intermediate

In this course you will learn the definition of a transaction, identify the situation in which a transaction is occurring, identify the transaction property that is violated in a specified situation., match various transaction participants with the tasks performed by them, match the components of a transaction with the tasks performed by them, match the problems that occur when multiple transactions simultaneously access a database with the situations in which they occur, identify the transaction problem that is solved by a specified isolation level, and identify the situations in which distributed transactions are used. Other topics include:

- Labeling the process boxes in a flowchart with the steps involved in the two-phase commit approach used to manage distributed transactions.
- Sequencing the steps to run a container-managed transaction.
- Matching various transaction attribute values with the scopes that they provide to a business method.
- Identifying the methods of the interfaces of the enterprise bean types for which the transaction attribute value must be specified.
- Identifying the conditions in which a container-managed transaction rolls back.
- Matching the methods of the UserTransaction interface used to manage a bean-managed transaction with their functions.
- Identifying the scope provided to the various types of enterprise beans in a bean-managed transaction.
- Identifying the functions of the Session Synchronization interface.
- Matching the methods of the Session Synchronization interface with their functions.

3.60 Troubleshooting Local Area Networks

Duration: 2 Hours

Level: Intermediate

In this course you will learn to identify the basic service and support tasks that are performed by a network administrator, label a scenario with the type of patch that is to be used, sequence the steps of the troubleshooting model, identify the checks carried out by a network administrator to provide a quick fix solution for the problem in a specific scenario, and prioritize the hypotheses derived to diagnose a network problem in a specific scenario by labeling. Other topics include:

- Identifying the tasks that need to be performed when executing a plan to solve a network problem.
- Identifying the tasks to prevent the recurrence of a network problem in a specific scenario.
- Identifying the step that should be performed according to the troubleshooting model to solve a problem in a specified scenario.
- Labeling a scenario with the type of LAN documentation practice that is used in specified scenarios.
- Labeling a scenario with the indicator that is to be used in the scenario.
- Labeling a scenario with the troubleshooting tool that is to be used in the specified scenario.
- Network problems that can be diagnosed using a LAN analyzer.
- Labeling the tools used for resolving network equipment problems with their uses.

Prerequisite: "Securing Local Area Networks"

3.61 Understanding Kerberos

Duration: 2 Hours

Level: Intermediate

In this course you will learn to identify the functions of Kerberos and encryption methods used in Kerberos, sequence the steps in the Kerberos authentication process, identify the naming styles for Kerberos realms, and match the Kerberos principal name-type with its use. Other topics include:

- Matching the Kerberos ticket flag with its function.
- The attributes of cross-realm operation.
- Sequencing the steps in obtaining credentials from the Authentication Server.
- Sequencing the steps to mutually authenticate a Kerberos client and a Kerberos server.

3.62 User Account and File System Security

Duration: 2 Hours

Level: Intermediate

In this Unix- and Windows NT-based course, you will learn to identify the passwords that should be used in a specified scenario, identify the command to implement password aging, the command to monitor logon attempts in a specified scenario, and the commands to verify account details. You will also learn to identify the umask command and the chmod command to be used in the specified situation. Other topics include:

- Applying a strong password by modifying the registry.
- Identifying the commands to verify account details.
- Renaming a specified account by using the User Manager for Domains utility.
- Applying an account policy by using the User Manager for Domains utility.
- Assigning share permissions in a specified situation.
- Assigning NTFS permissions on files and folders by using the Security tab.
- Matching the ls commands with the situations in which they are used.

3.63 Virus Protection and Recovery

Duration: 1 Hour

Level: Beginning

In the Virus Protection and Recovery course you will learn to identify the operations performed by the virus scanner, select the operations of memory scanners, identify the operations of the integrity checkers, and select the strategies used to prevent a virus from infecting a computer. Other topics include:

- Identifying the statements that describe a behavior blocker.
- Identifying the statements that describe heuristic scanners.
- Sequencing the steps to remove a virus.

3.64 Windows 2000 Security Management

Duration: 1 Hour

Level: Intermediate

In this course you will learn to identify the guidelines for selecting an appropriate certification management strategy and select and analyze appropriate certification management strategies that meet specified business requirements. Other topics include:

- Guidelines for designing an appropriate Proxy server management strategy.
- Selecting an appropriate Proxy server management strategy that meets specified business requirements.
- Analyzing Proxy server management strategies that are used to meet various business requirements.

Prerequisite: "Microsoft Proxy Server Security Features"

3.65 Windows NT Networking: Multiple Domains

Duration: 2 Hours

Level: Advanced

In this course you will learn to identify the features of the different types of trust relationships, establish a one-way trust relationship between two domains by using User Manager for Domains, identify the guidelines to be used for implementing groups across trusting and trusted domains, identify the features of a single and single master domain model, and identify the features of a multiple master and complete trust domain model. Other topics include:

- The advantage of the NDS name space structure over the NTDS name space structure.
- The advantages of NDS schema extensibility over NTDS schema extensibility.
- The advantages of NDS distributed architecture over NTDS distributed architecture.
- The advantages of NDS network security over NTDS network security.
- The advantages of the NDS authentication process NDS over the NTDS authentication process.
- The advantages of NDS network management features over NTDS network management features.
- The features of NDS and ADS.

4.0 Glossary

Note: The following terms are defined for use throughout this document.

Acceptable Risk — the level of *Residual Risk* that has been determined to be a reasonable level of potential loss/disruption for a specific IT system. (See *Total Risk*, *Residual Risk*, and *Minimum Level of Protection*.)

Accreditation — also known as *authorize processing* (OMB Circular A-130, Appendix III), and *approval to operate*. Accreditation (or authorization to process information) is granted by a management official and provides an important quality control. By accrediting a system or application, a manager accepts the associated risk. Accreditation (authorization) must be based on a review of controls. (See *Certification*.)

Acquisition, Development, and Installation Controls — the process of assuring that adequate controls are considered, evaluated, selected, designed, and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation, and operation stages.

Adequate Security — security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, acquisition, development, installation, operational, and technical controls.

Application — the system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications.

Approval to Operate — see *Certification* and *Accreditation*.

Automated Information System Security — synonymous with *Information Technology Security*.

Automated Information System Security Program — synonymous with *IT Security Program*.

Availability — the timely, reliable access to data and information services for authorized users.

Awareness — a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure.

Awareness, Training, and Education Controls — include (1) awareness programs which set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure, (2) training which teaches people the skills that will enable them to perform their jobs more effectively, and (3) education which is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities.

Baseline Security — the minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.

Behavioral Outcome — what an individual who has completed the specific training module is expected to be able to accomplish in terms of IT security-related job performance.

Certification — a formal process for testing components or systems against a specified set of security requirements. Certification is normally performed by an independent reviewer rather than one involved in building the system. Certification *can be* part of the *review of security controls* identified in OMB Circular A-130, Appendix III, which calls for security reviews to assure that management, operational, and technical controls are appropriate and functioning effectively. (See *Accreditation*.)

Computer Security — synonymous with *Information Technology Security*.

Computer Security Program — synonymous with *IT Security Program*.

Confidentiality — the assurance that information is not disclosed to unauthorized individuals or processes.

Education — IT security education focuses on developing the ability and vision to perform complex, multi-disciplinary activities and the skills needed to further the IT security profession. Education activities include research and development to keep pace with changing technologies and threats.

FISSEA — the *Federal Information Systems Security Educator's Association*, an organization whose members come from federal agencies, industry, and academic institutions devoted to improving the IT security awareness and knowledge within the federal government and its related external workforce.

Information Sharing — the requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.

Information Systems Security — synonymous with *IT Security*.

Information Systems Security Program — synonymous with *IT Security Program*.

Information Technology (IT) — computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data. IT components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware and software. See also *IT System* and *IT Security*.

Integrity — the quality of an IT system that reflects the logical correctness and reliability of the operating system; the logical completeness of the hardware and software that implements the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

IT Security — technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. Synonymous with *Automated Information System Security*, *Computer Security* and *Information Systems Security*.

IT Security Basics — a core set of generic IT security terms and concepts for all federal employees as a baseline for further, role-based learning.

IT Security Body of Knowledge Topics and Concepts — a set of 12 high-level topics and concepts intended to incorporate the overall body of knowledge required for training in IT security.

IT Security Literacy — the first solid step of the IT security training level where the knowledge obtained through training can be directly related to the individual's role in his or her specific organization.

IT Security Program — a program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information technology systems. Synonymous with *Automated Information System Security Program*, *Computer Security Program*, and *Information Systems Security Program*.

IT System — a collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating procedures. An IT system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected.

Job Function — the roles and responsibilities specific to an individual, not a job title.

Knowledge Levels — verbs that describe actions an individual should be capable of performing on the job after completion of the training associated with the cell. The verbs are identified for three training levels: Beginning, Intermediate, and Advanced.

Laws and Regulations — federal government-wide and organization-specific laws, regulations, policies, guidelines, standards, and procedures mandating requirements for the management and protection of information technology resources.

Learning — knowledge gained by study (in classes or through individual research and investigation).

Learning Continuum — a representation in which a common characteristic of learning is presented as a series of variations from awareness through training to education.

Learning Objective — a link between the verbs from the "knowledge levels" section to the "Behavioral Outcomes" by providing examples of the activities an individual should be capable of doing after successful completion of training associated with the cell. Learning Objectives recognize that training must be provided at Beginning, Intermediate, and Advanced levels.

Likert Scale — an evaluation tool that is usually from one to five (one being very good; five being not good, or vice versa), designed to allow an evaluator to prioritize the results of the evaluation.

Management Controls — management controls are actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions.

Minimum Level of Protection — the reduction in the *Total Risk* that results from the impact of in-place safeguards. (*See Total Risk, Acceptable Risk, and Residual Risk.*)

Operational Controls — the day-to-day procedures and mechanisms used to protect operational systems and applications. Operational controls affect the system and application environment.

Performance-Based — a method for designing learning objectives based on behavioral outcomes, rather than on content that provides benchmarks for evaluating learning effectiveness.

Residual Risk — the potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards. (See *Total Risk, Acceptable Risk, and Minimum Level of Protection.*)

Risk — the probability that a particular security threat will exploit a system vulnerability.

Risk Management — the on-going process of assessing the risk to IT resources and information, as part of a risk-based approach used to determine adequate security for a system, by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Roles and Responsibilities — functions performed by someone in a specific situation and obligations to tasks or duties for which that person is accountable.

Role-Based — mapped to job function, assumes that a person will take on different roles, over time, within an organization and different responsibilities in relation to IT systems.

Sensitivity — the degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components.

System — see *IT System*.

System Environment — the unique technical and operating characteristics of an IT system and its associated environment, including the hardware, software, firmware, communications capability, organization, and physical location.

System Interconnection — the requirements for communication or interconnection by an IT system with one or more other IT systems or networks, to share processing capability or pass data and information in support of multi-organizational or public programs.

Technical Controls — hardware and software controls used to provide automated protection to the IT system or applications. Technical controls operate within the technical system and applications.

Threat — an activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Total Risk — the potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). (See *Acceptable Risk, Residual Risk, and Minimum Level of Protection.*)

Training — teaching people the knowledge and skills that will enable them to perform their jobs more effectively.

Training Assessment — an evaluation of the training efforts.

Training Effectiveness — a measurement of what a given student has learned from a specific course or training event, i.e., learning effectiveness; a pattern of student outcomes following a specific course or training event; i.e., teaching effectiveness; and the value of the specific class or training event, compared to other options in the context of an agency's overall IT security training program; i.e., program effectiveness.

Training Effectiveness Evaluation — information collected to assist employees and their supervisors in assessing individual students' subsequent on-the-job performance, to provide trend data to assist trainers in improving both learning and teaching, and to be used in return-on-investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of IT security

awareness, security literacy, training, and education options for optimal results among the workforce as a whole.

Training Matrix — a table that relates role categories relative to IT systems—Manage, Acquire, Design and Implement, Operate, Review and Evaluate, and Use (with a seventh category, "other" included to provide extensibility) with three training content categories Laws and Regulations, Security Program, and System Life Cycle Security.

Vulnerability — a flaw or weakness that may allow harm to occur to an IT system or activity.